VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

DIGITÁLNÍ STEGANOGRAFIE A STEGOANALÝZA

DIGITAL STEGANOGRAPHY AND STEGANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE **TOMÁŠ POREMBA**
AUTHOR

VEDOUCÍ PRÁCE **Ing. JOSEF STRNADEL, Ph.D.**
SUPERVISOR

BRNO 2018

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav počítačových systémů Akademický rok 2017/2018

Zadání diplomové práce

Řešitel: **Poremba Tomáš, Bc.**
Obor: Bezpečnost informačních technologií
Téma: **Digitální steganografie a stegoanalýza**
Digital Steganography and Steganalysis
Kategorie: Bezpečnost

Pokyny:

1. Podrobně klasifikujte metody z oblastí digitální steganografie a stegoanalýzy, shrňte klíčové pojmy, principy a vlastnosti související s metodami a současný stav ve zmíněných oblastech.
2. Zvolte typ skrývané informace (textová, obrazová apod.) a její vlastnosti. Na základě existující či vlastní analýzy způsobů ukládání dat a typu skrývané informace zužte a zvolte vhodné způsoby pro ukládání dat a vhodné metody steganografie a stegoanalýzy.
3. Implementujte několik existujících metod steganografie vč. stegoanalýzy, zvažte jejich modifikace, popř. návrh a implementace vlastních metod.
4. Demonstrujte a vyhodnoťte funkčnost a vlastnosti implementovaných steganografických metod z hlediska skrývání resp. odkrývání zvoleného typu informace a detekce skryté informace prostředky stegoanalýzy.
5. Dosažené výsledky diskutujte, navrhněte možné návaznosti a rozšíření předloženého řešení.

Literatura:

- Dle pokynů vedoucího.

Při obhajobě semestrální části projektu je požadováno:

- Splnění bodů 1 a 2 zadání.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci dřívějších projektů (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Strnadel Josef, Ing., Ph.D.**, UPSY FIT VUT
Datum zadání: 1. listopadu 2017
Datum odevzdání: 23. května 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav počítačových systémů a sítí
612 66 Brno, Božetěchova 2

L.S.

prof. Ing. Lukáš Sekanina, Ph.D.
vedoucí ústavu

Abstrakt

Táto diplomová práca sa zaoberá problematikou digitálnej steganografie a stegoanalýzy. Približuje význam oboch odborov a ponúka krátky prehľad historického vývoja v danej oblasti. Práca podrobne rozdeľuje existujúce steganografické a stegoanalytické metódy a opisuje vlastnosti jednotlivých odvetví steganografie. Vzhľadom na zvolenú oblasť steganografie (obrazovú) práca zužuje výber vhodných steganografických a stegoanalytických metód, ktorých princípy detailne popisuje. Výsledky práce zahŕňajú experimentálne overenie vlastností vybraných steganografických metód a vyhodnotenie úspešnosti jednotlivých stegoanalytických metód pri odhaľovaní steganografie.

Abstract

This thesis deals with digital steganography and steganalysis. It explains the significance of both disciplines and gives a brief overview of the history in the given fields. The paper separates existing steganographic and steganalytic methods and describes the attributes of various branches of steganography. With respect to the chosen field of steganography (the image steganography), the paper narrows down the set of suitable steganographic and steganalytic methods, whose features are then described in detail. The results of the thesis inlcude experiments that verify the features of chosen steganographic methods and evaluation of steganalytic methods and their success in detection of steganography.

Kľúčové slová

steganografia, stegoanalýza, obrazová steganografia

Keywords

steganography, steganalysis, image steganography

Citácia

POREMBA, Tomáš. *Digitální steganografie a stegoanalýza*. Brno, 2018. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Josef Strnadel, Ph.D.

Digitální steganografie a stegoanalýza

Prehlásenie

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne pod vedením pána Ing. Josefa Strnadela, Ph.D. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Tomáš Poremba
22. mája 2018

Poďakovanie

Na tomto mieste by som rád poďakoval pánovi Ing. Josefovi Strnadelovi, Ph.D. za jeho odborné vedenie, cenné rady pri vypracovaní tejto práce a trpezlivosť a čas, ktorý mi venoval. Ďalej by som rád poďakoval svojej rodine za podporu počas celého štúdia.

Obsah

Zoznam obrázkov

Kapitola 1

Úvod

Už v antických časoch ľudia poznali cenu informácií a vedeli, že jej utajenie pred nepriateľom môže byť kľúčovým bodom v konfliktoch. V modernej dobe ľudia čoraz viac prikladajú význam vlastnému súkromiu a ochrane vlastných dát. Z týchto, ale aj ďalších dôvodov, začali vznikať postupy a metódy, ako tieto informácie ochrániť pred nepovolanými osobami. Nástupom kryptografie sa zvýšila ochrana informácií, ale práve steganografia priniesla možnosť utajiť nielen podstatu informácie, ale aj jej existenciu.

Existencia metód na skrývanie informácii so sebou priniesla zároveň snahu odhaliť prítomnosť týchto tajomstiev v inak bežnej komunikácii, či v na prvý pohľad obyčajných dátach. So steganografiou tak vznikla zároveň veda zaoberajúca sa práve odhaľovaním informácií skrytých možnosťami steganografie – stegoanalýza. Jej význam vzrastá hlavne v dnešnej dobe, keď sa boj s ilegálnymi aktivitami zaoberá nielen dešifrovaním komunikácie, ale aj jej samotným odhalením.

Táto práca sa zameriava na digitálnu steganografiu a stegoanalýzu. Postupne priblíži rozdelenie digitálnej steganografie a stegoanalýzy, klasifikuje metódy v jednotlivých odvetviach týchto disciplín a popíše jednotlivé vlastnosti spomenutých metód a ich využitie. Vysvetlenie pojmov spätých s problematikou a rozdelenie steganografie a stegoanalýzy sa nachádza v kapitole 2. Táto kapitola je prevzatá z autorovho semestrálneho projektu [15]. Ďalej práca zúži výber metód vzhľadom na typ skrývanej informácie – text – a vlastností uloženia skrývanej informácie a média, v ktorom sa bude informácia nachádzať – digitálne obrázky. Princípy a a porovnanie vlastností vybraných a implementovaných steganografických metód sú popísané v kapitole 3. Následne práca popíše spôsoby, akými je možné tieto metódy odhaliť. Popis stegoanalytických metód a experimentálne overenie ich funkčnosti pri odhaľovaní steganografie sa nachádza v kapitole 4. V poslednej kapitole čitateľ nájde popis prostriedkov využitých pri implementácii jednotlivých metód a spôsob, akým boli vybrané steganografické a stegoanalytické metódy implementované.

Kapitola 2

Digitálna steganografia a stegoanalýza

2.1 Pojem steganografia a stegoanalýza

Slovo steganografia je odvodené z gréčtiny a znamená "zakryté písmo". To vystihuje podstatu steganografie a odlišuje ju tak od kryptografie [14]. Podstatou steganografie ako techniky je totiž umožniť komunikujúcim stranám zatajiť existenciu tajnej správy v médiu, ktoré je voľne prístupné a nezabezpečené, a teda skryť komunikáciu v odpočúvateľnom médiu. Odosielateľ a prijímateľ potom spolu komunikujú bez toho, aby o tom niekto vedel. Efektívne vloženie správy do krycieho súboru je však náročné, a to z viacerých dôvodov. Steganografický proces (obr. 2.1) totiž musí brať do úvahy viaceré faktory, medzi ktoré patria [7]:

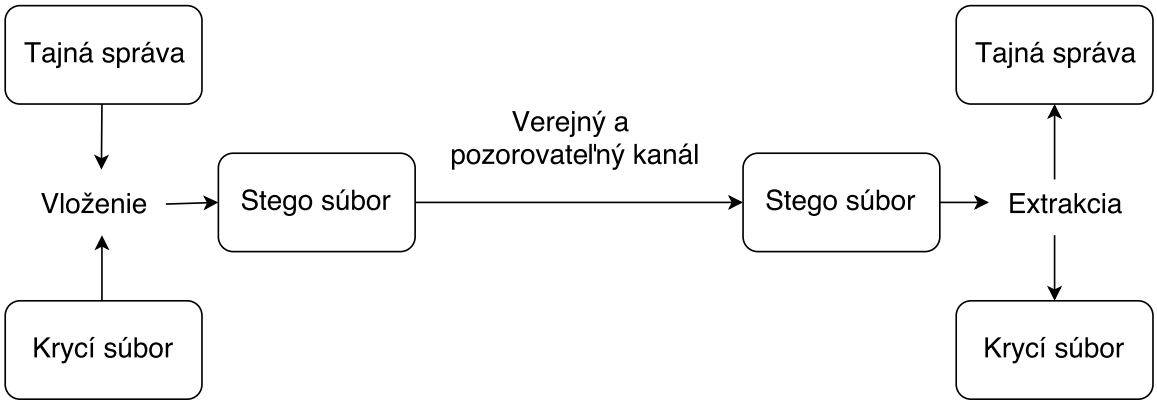
- nedetekovateľnosť,
- kapacita,
- robustnosť,
- odolnosť voči manipulácii.

Nedetekovateľnosť. Nedetekovateľnosť poukazuje na fakt, že skrytá informácia nemôže byť postrehnuteľná útočníkom. Táto vlastnosť je podstatným faktorom, ktorý musia steganografické postupy zaručiť na vysokej úrovni. Po odhalení prítomnosti skrytej informácie totiž steganografický proces zlyháva – nesplnil svoj účel.

Kapacita. Kapacita udáva množstvo informácie alebo dát, ktoré môžu byť vložené do krycieho súboru (média).

Robustnosť. Robustnosť udáva schopnosť steganografického procesu chrániť vloženú tajnú správu v krycom médiu pred znehodnotením kompresnými a dekompresnými procesmi aplikovanými na stegosúbor.

Odolnosť voči manipulácii. Odolnosť voči manipulácii ukazuje úroveň ochrany pred manipuláciou vloženej správy útočníkom. Môže ísť o upravenie tajnej správy alebo jej úplné odstránenie útočníkom v prípade jej detekcie.



Obr. 2.1: Základná schéma steganografického procesu.

Steganografia sa často spomína v súvislosti s kryptografiou. Tieto dve vedné disciplíny spolu úzko súvisia, no zároveň sa odlišujú v podstatných detailoch. Úlohou kryptografie je zatajenie obsahu komunikácie, naproti tomu úlohou steganografie je zatajenie komunikácie samotnej. To však nebráni tomu, aby bola kryptografia využívaná v steganografii. Celková bezpečnosť môže byť zvýšená šifrovaním tajnej informácie pred jej vložením do krycieho súboru.

Stegoanalýza je vedná disciplína zaoberajúca sa odhaľovaním tajných informácií a útokmi na stegoobjekty. Voči steganografii zastáva rovnakú úlohu, akú má kryptoanalýza voči kryptografii. Jej cieľom je odhaliť prítomnosť skrytej informácie, prípadne zistiť objem prenášanej informácie a v najlepších prípadoch zistiť aj samotnú informáciu. Stegoanalýza býva buď slepá, keď proces analýzy nepozná spôsob, akým bola prípadná tajná správa ukrytá, alebo cielená, keď je použitá steganografická metóda známa.

V tejto práci sa vyskytujú určité pojmy vzťahujúce sa k steganografii a stegoanalýze. Ich význam bude objasnený na nasledujúcich riadkoch.

Krycie médium. Krycie médium (súbor) je súbor, do ktorého je vložená skrytá informácia. Predstavuje krytie pre skrytú informáciu.

Tajná správa. Tajná správa predstavuje informáciu alebo dáta, ktorých existenciu chce odosielateľ utajiť pred okolitým svetom. Tajná správa je vložená do krycieho média.

Stegomédium. Stegoobjekt (súbor, médium) je tvorený krycím súborom, do ktorého bola vložená tajná správa. Je teda prostriedkom komunikácie v steganografii.

2.2 História steganografie a aktuálny stav

Pôvod steganografie môžeme hľadať už v antickom Grécku. Prvé zmienky hovoria o kamuflovaní správy do mŕtveho tela zajaca, ktorý mal predstavovať loveckú trofej. Tá bola prepravená mužom vydávajúcim sa za lovca, čo malo za úlohu znížiť podozrenie, že je poslom správy. Najčastejšou zmienkou z antického Grécka je však komunikácia pomocou voskových tabuliek. Tie boli tvorené základom z dreva, do ktorého bola vpísaná tajná správa. Následne bola takáto doska pokrytá voskom a vydávaná za nepoužitú voskovú tabuľku [14].

Objav pergamenu, ktorý sa dal využiť ako krycie médium, umožnil vznik nových techník steganografie. Spomeňme aspoň neviditeľný atrament – po napísaní správy a zaschnutí atrament zmizol, no po zohriatí pergamenu nad plameňom zhnedol a umožnil tak prečítať správu.

Vynález papiera v stredoveku viedol k veľkému pokroku v steganografii. Nové princípy a postupy viedli aj k používaniu vodoznakov. Dosah tohto prelomu je možné sledovať dodnes, keďže moderná digitálna obrazová steganografia využíva princípy odhalené už v tej dobe.

Tak ako v minulosti, tak aj v modernej dobe vynálezy ovplyvňujú steganografické trendy. Príchod počítačov a sietí podnietil vznik nových odvetví, ktoré sa dajú zhrnúť pod termín digitálna steganografia. Najmladším odvetvím digitálnej steganografie je sieťová steganografia, ktorej sa v poslednej dobe venuje zvýšená pozornosť, keďže odstraňuje určité nedostatky ostatných typov digitálnej steganografie.

2.3 Digitálna steganografia

Digitálna steganografia je súhrnný názov pre steganografické metódy a postupy aplikované na digitálne média (multimediálne, textové, spustiteľné či ostatné súbory, protokoly). Podľa typu krycieho média ju môžeme rozdeliť do nasledujúcich odvetví [14]:

- textová steganografia,
- multimediálna steganografia (ďalej rozdelená na obrazovú, zvukovú a video steganografiu),
- steganografia súborov,
- sieťová steganografia.

2.3.1 Textové metódy

Textová steganografia je azda najzložitejšou formou steganografie s ohľadom na faktory spomenuté v podkapitole 2.1. Textové dokumenty a ich štruktúra totiž neposkytujú redundanciu dát porovnateľnú s ostatnými multimediálnymi súbormi ako je zvuk, video či fotografia. Aj malé zmeny obsahu textového súboru sú teda oveľa viditeľnejšie ako napríklad v prípade zmien pár pixelov vo fotografii. Skrývanie tajnej správy v textových dokumentoch tak musí brať vysoký zreteľ na pôvodný obsah. Metódy textovej steganografie môžeme rozdeliť do troch kategórií:

- zmena významu textu,
- štatistické a náhodné generovanie textu – využíva generovanie náhodného krycieho textu na základe vlastností tajnej správy,
- zmeny formátu textu.

Najrozšírenejšou kategóriou sú metódy zaoberajúce sa zmenou formátu textu. Tie pracujú s obsahom textu (zmenou jednotlivých slov), samotným formátovaním textu (veľkosť a počet medzier medzi vysadenými znakmi) alebo využitím špecifík programovacích alebo značkovacích jazykov, ktoré predstavujú obsah daných súborov. Metódy, ktoré práca popisuje, sú spomenuté v [12].

Sémantická metóda. Sémantická metóda sa opiera o ukrytie informácie pomocou synoným. Zmena slov za ich synonymá môže ukrývať jeden alebo viacero bitov tajnej správy. Nahradenie jedným zo synoným tak predstavuje napríklad bitovú 1 a iným synonymom bitovú 0. Podobne môže fungovať metóda na základe hláskovania slov – ako príklad poslúži britská a americká angličtina. Tie sa v hláskovaní niektorých slov líšia (color – colour) a využitie rôznych variantov tak ukrýva bity tajnej správy.

Zmena zarovnania. Zmena zarovnania krycieho súboru môže ukrývať bitové 0 a 1 tajnej správy. Využívajú sa dva typy zarovnania – riadkovanie a zarovnanie slov. V prvom prípade sa pomocou bitov tajnej správy mení riadkovanie krycieho textu, v druhom prípade sa text delí na skupiny s rovnakým počtom slov a mení sa zarovnanie jedného slova v skupine.

Vkladanie bielych znakov. Ďalšou metódou je vkladanie bielych znakov. Biele znaky, ktoré značia bity tajnej správy, môžu byť vložené medzi jednotlivé slová alebo vety. Ďalej je možné využiť biele znaky na konci riadkov. Toto riešenie je nenápadné a môže uložiť väčšie množstvo informácie ako biele znaky medzi vetami. Ďalším miestom, na ktoré je možné uložiť biele znaky, je priestor medzi jednotlivými odstavcami. Tento spôsob umožňuje ukrytie najväčšieho množstva tajnej správy na jeden výskyt.

Vlastnosti vyššie spomenutých metód sa zásadne odvíjajú od štruktúry krycieho textu. Vo všeobecnosti platí, že zvýšenie kapacity znižuje nedetekovateľnosť. Dá sa vypozorovať, že pre textové metódy toto pravidlo neplatí len v rámci jednej metódy, ale aj medzi metódami. Sémantické metódy majú zo svojej podstaty nízku kapacitu, na druhú stranu sú veľmi náročne detekovateľné. Metódy založené na vkladaní bielych znakov alebo zarovnaní sa vyznačujú podstatne vyššou kapacitou, no za tú cenu, že zarovnanie pri priveľkých odchýlkach je ľahko odhaliteľné už bežným pohľadom a dlhé postupnosti bielych znakov v súbore sú odhaliteľné veľmi jednoduchou a rýchlou analýzou.

Vplyv štruktúry krycieho textu na kapacitu je najzreteľnejší pri výbere metódy vkladania bielych znakov. Označme si *výskyt* ako miesto, na ktorom sa môže nachádzať biely znak. Potom *kapacita na miesto* určuje koľko bielych znakov môžeme do daného výskytu umiestniť tak, aby to bolo relatívne nespozorovateľné. Zhrnutie hodnôt týchto dvoch atribútov je v tabuľke 2.1. Štruktúrovaný text s ohľadom na vysoké množstvo odstavcov zvýši kapacitu krycieho textu. Zarovnanie textu do bloku prakticky eliminuje možnosť využitia vkladania znakov na konce riadkov. Výber vhodnej metódy vzhľadom na štruktúru je tak kľúčový, ak chceme zabezpečiť nízku pravdepodobnosť odhalenia tajnej správy.

metóda vloženia bielych znakov	výskyt	kapacita na výskyt
medzi slovami	vysoký	nízka
medzi vetami	stredný	nízka
konce riadkov	stredný	stredná
konce paragrafov	nízky	vysoká

Tabuľka 2.1: Atribúty vzťahujúce sa ku kapacite metód založených na vkladaní bielych znakov.

2.3.2 Obrazové metódy

Obrazová steganografia sa zameriava na slabú schopnosť ľudského oka rozoznávať malé zmeny v krycom obraze, snaží sa oklamať ľudské vnímanie a presvedčiť človeka, že s krycím obrazom nebolo nijako manipulované. Obrazové metódy digitálnej steganografie môžeme podľa časti digitálnej snímky využitej na ukrytie tajnej správy rozdeliť na nasledujúce kategórie [5]:

- metódy využívajúce formát súboru,
- metódy priestorovej domény,
- metódy frekvenčnej domény,
- adaptívne metódy, perceptuálne maskovanie.

Využitie formátu súboru
Najmenšou skupinou metód s najnižším uplatnením sú metódy využívajúce prostriedky poskytnuté formátom súboru, v ktorom je samotná obrazová snímka uložená. Tieto metódy sa vyznačujú vysokou kapacitou ako bude zrejmé z uvedených príkladov nižšie. Bezpečnosť týchto metód a ich nedetekovateľnosť je veľmi nízka.

Príkladom môže byť využitie priestoru za EOF v súboroch formátu JPEG. Správa ľubovoľnej dĺžky je zapísaná na koniec súboru za znak EOF. Túto správu nerozpoznajú aplikácie pracujúce s obrazovými snímkami, no je ľahko detekovateľná akýmkoľvek textovým editorom. Ďalším miestom na uloženie tajnej správy môžu byť metadáta určené na záznam o prístroji, ktorý vyhotovil danú snímku (EXIF). Výhodou týchto metód je, že nijakým spôsobom neovplyvňujú kvalitu snímky, na druhej strane sú veľmi ľahko detekovateľné a napadnuteľné.

Metódy v priestorovej doméne
Najvyužívanejšími metódami obrazovej steganografie sú tie, ktoré sa zaoberajú zmenou priestorovej domény snímok. Jednou z kategórií sú metódy substitučného charakteru, u ktorých dochádza k zámene bitov v obrazových dátach. Na tento účel sú použité najmenej významné bity. Odtiaľ pochádza aj súhrnný názov týchto metód – LSB (Least Significant Bits).

LSB metódy majú viacero variantov, líšia sa aj v počte použitých bitov. Vo všeobecnosti platí, že čím menej bitov je zamenených, tým menšia zmena v obraze nastáva, a tým náročnejšie je odhaliť tajnú správu. Použitím viacerých bitov však stúpa kapacita krycieho obrazu, čo potvrdzuje pravidlo spomenuté pri textových metódach.

Najjednoduchším variantom LSB je nahradenie určitého pevne stanoveného počtu najmenej významných bitov pixelov krycieho obrázku tajnou správou. Táto metóda vykazuje vysokú kapacitu a veľmi jednoduchú implementáciu. Nehodí sa však pre jeden z najpoužívanejších obrazových formátov – JPEG.

Zmenu hodnoty pixelu o 1, podobne ako metóda LSB s jedným bitom, využíva aj metóda ± 1 vkladania. Tá však na rozdiel od metódy LSB umožňuje aj zníženie hodnoty párneho pixelu, či zvýšenie hodnoty nepárneho, čo má za následok nižšiu detekovateľnosť tajnej správy vďaka menšiemu ovplyvneniu histogramu snímky.

Metódy vo frekvenčnej doméne
Príchod LSB metód znamenal veľký pokrok v obrazovej steganografii, no tieto metódy sú

ľahko napadnuteľné. Našli si však uplatnenie aj v metódach zaoberajúcich sa frekvenčnou doménou. Hlavným predstaviteľom týchto metód je metóda založená na DCT kompresii JPEG snímok – algoritmus JSteg. Dáta tajnej správy sa ukladajú do koeficientov DCT. Tento proces však vyžaduje opatrnosť pri zmene koeficientov, keďže tieto ovplyvňujú blok pixelov stegoobrázka a nesprávny výber koeficientov môže zanechávať artefakty (rozostrenie obrazu, nápadná zmena farebnosti a iné). Varianty tohto algoritmu zahŕňajú pseudonáhodný výber menených koeficientov alebo zmenu iba nenulových koeficientov.

Adaptívna steganografia
Adaptívne metódy sú špeciálnym prípadom vyššie spomenutých metód. Základným prvkom je skúmanie globálnych štatistických vlastností snímky. Na ich základe sa potom pristupuje k zmene najmenej významných bitov či výberu správnych DCT koeficientov. Tieto metódy využívajú obrázky s vysokou dávkou šumu (buď vloženého alebo prirodzeného), pretože sa opierajú o oblasti s vysokou lokálnou štandardnou odchýlkou.

Jednoduchým príkladom týchto metód je variant LSB metódy – metóda susedov. Tá využíva určité okolie pixla na odhalenie variácie v obraze. Ak sa pixely líšia vo veľkej miere, môžu byť využité na uloženie tajnej správy – nebudú totiž vytvárať veľký šum.

Iné metódy využívajú k uloženiu informácie napríklad okolia hrán, keďže tieto miesta vykazujú vysokú členitosť a vkladanie informácie tak nebude mať vysoký vplyv na zvyšovanie šumu.

2.3.3 Zvukové metódy

Zvuková steganografia (taktiež audio steganografia) je založená na podobnom princípe ako steganografia obrazová. Hlavným princípom je odhalenie redundantných častí krycieho objektu, ktorých prípadná zmena nevzbudí podozrenie na prítomnosť tajnej správy. Tieto zmeny potom reprezentujú samotnú tajnú správu. Metódy audio steganografie zahŕňajú [10]:

- LSB,
- paritné kódovanie,
- fázové kódovanie,
- rozprestretie spektra,
- skrývanie echa.

LSB. LSB v audio súboroch funguje na rovnakom princípe ako LSB v obrazovej steganografii. Vo vzorkách audio signálu je zmenený najmenej významný bit podľa bitov tajnej správy.

Paritné kódovanie. Metóda paritného kódovania pracuje podobne ako metóda LSB. Avšak namiesto jednotlivých vzoriek berie do úvahy dlhšie oblasti signálu. Porovnáva paritu danej oblasti s bitom tajnej správy, ktorý má byť uložený. Ak bit nesúhlasí, zmení sa ľubovoľný bit v oblasti, a tým pádom aj parita. Táto technika je robustnejšia ako LSB a poskytuje väčší priestor pre bitovú zmenu. Samozrejme, jej kapacita je nižšia ako kapacita techniky LSB.

Fázové kódovanie. Fázové kódovanie nahrádza fázovú komponentu malej časti pôvodného signálu referenčnou fázou, ktorá predstavuje skrytú informáciu.

Rozprestreté spektrum. Metóda rozprestretého spektra rozdelí tajnú informáciu naprieč frekvenčným spektrom. Vyznačuje sa vysokou odolnosťou voči rušeniu, no táto metóda má voči ostatným nedostatok v zanesení relatívne vysokého šumu do krycieho signálu.

Skrývanie echa. Technika skrývania echa ukladá tajnú informáciu ako ozvenu v pôvodnom signále, podľa možnosti nerozoznateľnú ľudským sluchom. Krycí signál je rozdelený do blokov, ktorých počet korešponduje s dĺžkou správy. V každom bloku je potom echo zakódované s parametrami určujúcimi či je ukrytá bitová 0 alebo 1. Táto technika je najrobustnejšia zo spomenutých audio steganografických metód.

2.3.4 Steganografia pomocou súborov a súborových systémov

Steganografia pomocou súborov môže mať viacero podôb. Prvá je skrývanie tajnej informácie do spustiteľných súborov. Spustiteľné súbory sú tvorené postupnosťou strojových inštrukcií. Zjednodušene sa dajú chápať ako slová textu. Túto vlastnosť využíva metóda podobná sémantickej textovej metóde založenej na synonymách. Výber rôznych ekvivalentných inštrukcií tak môže ukrývať bitovú postupnosť tajnej správy. Výber ekvivalentných inštrukcií však nie je jedinou možnosťou ako pozmeniť strojový kód programu. Permutácie postupnosti na sebe nezávislých inštrukcií môžu reprezentovať bitovú postupnosť a zakódovať tak tajnú správu. Posledná použitá technika v spustiteľných súboroch je radenie reťazcov inštrukcií. V tejto technike záleží na ekvivalencii reťazcov inštrukcií, ktoré sú usporiadané do tried podľa ekvivalencie. Pri kódovaní tajnej správy sa vyberie reťazec z množiny reprezentujúcej skrývanú postupnosť bitov. Od počtu tried ekvivalentných reťazcov závisí množstvo informácie, ktoré vieme skryť pod jeden reťazec [1].

Ďalšia technika, ktorá náleží do tejto oblasti, je steganografický súborový systém. Jeho hlavným prínosom je analógia s neviditeľným atramentom. Súborový systém v tomto prípade zodpovedá náhodnej postupnosti bitových núl a jednotiek. Táto postupnosť sa len nepatrne odlišuje od bežne sa vyskytujúceho šumu na prázdnom médiu a iba ten, kto daný systém vytvoril a spätne extrahoval vektory označujúce hranice súborov, mohol aj s daným systémom pracovať. Steganografický súborový systém tak zahaľoval prítomnosť akýchkoľvek zmysluplných dát [14].

2.3.5 Video metódy

Video steganografia ťaží z poznatkov audio a obrazovej steganografie. Existujúce metódy kombinujú metódy audio a obrazovej steganografie a zvyšujú ich kapacitu. Video a kodeky, ktoré s ním pracujú, však poskytujú ďalší priestor pre skrytie tajnej správy. Bežne používaný kodek H.264 napríklad svojimi vlastnosťami umožňuje mapovanie bitov skrytej správy. Toto mapovanie môže byť aplikované na použité módy predikcie v snímkach alebo na pohybové vektory.

2.3.6 Sieťové metódy

Sieťová steganografia je najmladším odvetvím digitálnej steganografie. Práve jej je v poslednom čase venovaná zvýšená pozornosť, keďže prináša riešenie problémov steganografie v multimédiách. Tie dovoľujú ukrytie iba obmedzeného množstva informácie na jeden

súbor a samotné stegosúbory sú relatívne ľahko prístupné, a teda podrobiteľné stegoanalýze. Naproti tomu princípy sieťovej steganografie umožňujú dlhodobý, pomalý prenos dát s ohľadom na čas. Prístupnosť stegomédia je obmedzená, a pokiaľ nie je zachytená úplná sieťová komunikácia, detekcia tajnej správy je nemožná. Tieto dva fakty predurčujú sieťovú steganografiu k veľkému budúcemu využitiu, keďže jej odhalenie a eliminácia zo siete je podstatne náročnejšia ako pri multimediálnych dátach – odolnosť steganografických metód voči manipulácii je bezkonkurenčne najvyššia za predpokladu, že útočník nechce prerušiť, či zásadným spôsobom ovplyvniť funkčnosť komunikačného kanálu.

Metódy sieťovej steganografie vo väčšine prípadov využívajú skryté i známe medzery v návrhoch sieťových protokolov či známe nedostatky použitých princípov. Následné rozdelenie a popis jednotlivých metód je založený na [14].

Prvou využívanou medzerou je, podobne ako v multimediálnych súboroch, neschopnosť človeka odhaliť malé odchýlky medzi na prvý pohľad rovnakými objektami (stegoobjektami). Druhou je odosielanie stegoobjektov sieťou bez toho, aby ich zaregistrovali jednotlivé uzly prenášajúce komunikáciu. Využíva tzv. štatistickú neviditeľnosť – vytvorené anomálie, ktoré zabezpečujú skrytú komunikáciu, sa nevyskytujú v množstve prekračujúcom hranicu bežne sa vyskytujúcich anomálií.

Sieťová steganografia je založená na troch princípoch sprevádzajúcich sieťovú komunikáciu:

- chyby prenosového kanálu,
- redundancia informácií,
- neúplná definícia protokolu.

Chyby prenosového kanálu. Komunikačný kanál nie je takmer nikdy perfektný. Dochádza na ňom k rušeniu alebo stratám. Tento fakt môže byť využitý na to, aby sa zaň skrylo úmyselné poškodenie PDU (z angl. protocol data unit), jeho nedoručenie alebo iná manipulácia s prenosom.

Redundancia informácií. Väčšina protokolov nesie so sebou istú redundanciu prenášaných dát. Napríklad polia v hlavičkách môžu byť využité na skrytie prenášanej informácie za predpokladu, že to neovplyvní funkčnosť daného protokolu.

Neúplná definícia protokolu. Nie každý protokol je plne definovaný. Niektoré špecifikácie dovoľujú určitú voľnosť implementácie a tá môže byť zneužitá na ukrytie tajnej informácie.

Metódy sieťovej steganografie môžeme na základe toho, koľko protokolov využívajú, rozdeliť do dvoch veľkých kategórií: intra-protokolových a inter-protokolových. Toto rozdelenie je znázornené na obrázku 2.2.

Inter-protokolové metódy kombinujú zraniteľnosti dvoch a viacerých protokolov. Tieto protokoly môžu byť využívané na samotné ukrytie tajnej správy alebo môžu niesť rozdielny typ informácií. Príkladom môže byť metóda MLS (Multi-Level Steganography), ktorá delí prenos na rôzne hladiny. Vyššia hladina môže prenášať samotnú tajnú správu, nižšia zasa pomocnú informáciu pre prijímateľa. Tou môže byť kľúč, ktorým bola šifrovaná tajná správa, hash tajnej správy na overenie pravosti tajnej správy a pod. Metóda PadSteg pre zmenu využíva vlastnosť spojenia viacerých protokolov, konkrétne doplnenie ethernetových rámcov

nenulovým obsahom (tajnou správou), ak je využitý konkrétny protokol – ARP na odhalenie uzlov, ktoré sa zúčastnia tajnej komunikácie, TCP, UDP a ICMP na prenos samotnej správy. Pri prenose tajnej správy túto delí medzi spomenuté protokoly na sťaženie detekcie.

Intra-protokolové metódy využívajú na ukrytie tajnej správy iba jeden protokol. Môžeme ich rozdeliť do ďalších troch kategórií podľa toho, na akom princípe skrývajú tajnú informáciu. Toto rozdelenie je popísané v nasledujúcich riadkoch.

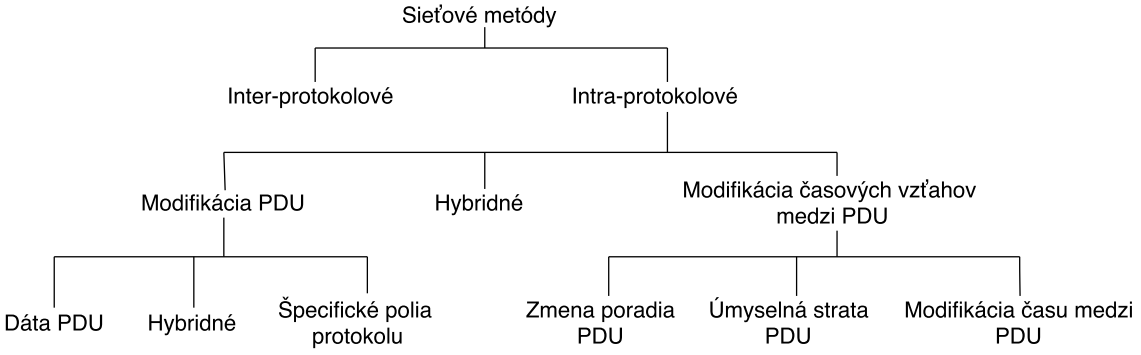
Metódy založené na modifikácii PDU
Metódy založené na modifikácii PDU využívajú samotný dátový obsah na uschovanie tajnej správy. Podľa modifikovanej časti PDU sa ďalej delia na metódy:

- založené na dátovom obsahu PDU,
- založené na špecifických poliach protokolu v PDU,
- zmiešané.

Metódy založené na časových vzťahoch medzi PDU
Ako názov napovedá, tieto metódy využívajú časové vzťahy medzi PDU a ich zmenu na prenesenie tajnej správy. Podľa typu časovej manipulácie sa ďalej delia na metódy:

- zmeny poradia odoslaných PDU,
- využívajúce úmyselnú stratu PDU,
- úmyselnú manipuláciu s časovým oneskorením jednotlivých PDU.

Hybridné intra-protokolové metódy
Tieto metódy využívajú tak modifikáciu samotného PDU, ako aj úpravu časových vzťahov medzi jednotlivými PDU. Sú kombináciou dvoch predchádzajúcich skupín, no stále využívajú a manipulujú iba s jedným protokolom.



Obr. 2.2: Rozdelenie sieťových steganografických metód.

2.4 Stegoanalýza

Pod pojmom stegoanalýza rozumieme proces útoku na potenciálny stegoobjekt. Stegoanalýza sa zameriava na detekciu štatistických odchýlok stegoobjektov s ohľadom na známe

vlastnosti podobných objektov. Krycie objekty bez ukrytej tajnej správy nesú predvídateľné charakteristiky, naproti tomu stegoobjekty sa vyznačujú určitou odchýlkou. Techniky stegoanalýzy môžeme rozdeliť na dve skupiny. Prvou je cielená stegoanalýza, ktorá sa zaoberá špecifickou steganografickou metódou. Táto technika je veľmi efektívna pri útoku na stegoobjekty, na ktoré je zameraná, avšak akákoľvek iná steganografická metóda pre ňu predstavuje neprekonateľnú prekážku.

Druhou skupinou sú modernejšie slepé stegoanalytické metódy. Nezameriavajú sa na špecifickú metódu a sú schopné odhaliť prítomnosť tajnej správy aj bez znalosti použitej steganografickej metódy. Tieto metódy však nevedia odhaliť použitú steganografickú metódu, ak nie sú trénované sadou, ktorá by ich obsahovala. V drvivej väčšine príkladov sú založené na strojovom učení [13].

Vo všeobecnosti môžeme stegoanalytické techniky na základe množstva hľadanej informácie rozdeliť do nasledujúcich kategórií [6]:

- odhalenie prítomnosti tajnej správy,
- identifikácia použitej metódy,
- určenie dĺžky tajnej správy,
- identifikácia miest nesúcich tajnú správu,
- extrakcia tajnej správy.

Stegoanalytické metódy sa od seba líšia spôsobom detekcie prítomnosti tajnej správy. Na základe použitého princípu sa dajú rozdeliť na dve kategórie: štatistická stegoanalýza a stegoanalýza založená na extrakcii rysov.

Štatistická stegoanalýza. Táto forma stegoanalýzy využíva na odhalenie tajnej správy zmenu štatistických vlastností obrazu. Tieto vlastnosti môžu byť prvého radu (napríklad histogram intenzít v sivotónovom obrázku) alebo vyššieho radu (vlastnosti dvojíc či trojíc susedných pixelov). Použitie štatistík vyššieho radu je v odhaľovaním steganografie efektívnejšie, no zároveň aj náročnejšie, keďže vyžadujú podstatne vyššiu dimenzionalitu.

Stegoanalýza na základe extrakcie rysov. Extrakcia rysov sa zameriava na izoláciu a identifikáciu rôznych štatistických vlastností. Snaží sa o výber takých rysov, ktoré najlepšie reprezentujú daný obrázok. Analýza týchto rysov potom vedie k odhaleniu tajnej správy. Často využívaným postupom je trénovanie klasifikátorov pomocou extrahovaných rysov.

Kapitola 3

Metódy obrazovej steganografie

V dnešnej dobe existujú dve široké oblasti v obrazovej steganografii, ktoré sú reálne využívané: steganografia v priestorovej doméne a steganografia vo frekvenčnej doméne. Metódy oboch typov využívajú vlastnosti algoritmov, ktoré sú používané na zakódovanie a uloženie informácií do rôznych obrazových formátov. Prvá skupina formátov využíva na uloženie obrazových dát priamo hodnoty pixelov (v pôvodnej alebo komprimovanej podobe). Medzi formáty pracujúce s priestorovou doménou patria napríklad BMP, GIF alebo PNG. Druhou skupinou sú potom formáty využívajúce frekvenčnú doménu. Obrazové informácie nie sú ukladané pixel po pixeli, no sú z priestorovej domény transformované rôznymi technikami (napríklad diskrétnou kosínusovou transformáciu v JPEG) do frekvenčnej domény. Steganografické metódy potom na uloženie skrytej informácie nevyužívajú pixely pôvodného obrazu, ale zameriavajú sa na použité transformačné algoritmy a ich parametre. Príkladom môže byť ukrytie bitov skrytej správy v koeficientoch DCT (z angl. discrete cosine transform) pomocou LSB princípu, ktoré sa používajú pri kompresii vo formáte JPEG.

3.1 Typ skrývanej informácie

Zvoleným typom skrývanej informácie pre potreby tejto práce je text. Textové súbory umožňujú uloženie dostatočného množstva informácie už pri veľmi malých veľkostiach súborov. Ďalej sú textové súbory dobre komprimovateľné a dovoľujú tak ďalej zvýšiť kapacitu použitých steganografických algoritmov.

3.2 Popis obrazových formátov

Podľa rozdelenia obrazových metód je pochopiteľné, že jednotlivé metódy budú aplikovateľné iba na určité formáty. Pre obe kategórie bude použitý jeden formát obrazových dát, ktorý bude túto skupinu reprezentovať. Pre formáty ukladajúce údaje v priestorovej doméne to bude formát PNG a pre formáty zaoberajúce sa frekvenčnou doménou to bude JPEG.

PNG
Formát PNG (Portable Network Graphics) je obrazový rastrový formát podporujúci bezstratovú kompresiu dát. Bol vyvinutý ako náhrada formátu GIF a je jedným z najpoužívanejších obrazových formátov na internete. Tento formát bol navrhnutý ako ľahko implementovateľný, používa iba voľne dostupné algoritmy a prináša veľmi dobrú kompresiu dát. Oproti formátu GIF je formát PNG robustnejší voči neodhaleným útokom a najväč-

ším prínosom je prítomnosť úplného alfa kanálu, ktorý umožňuje variabilnú priehľadnosť v obrázkoch [2]. Zároveň však zachováva dôležité vlastnosti formátu GIF – medzi inými postupné zobrazovanie a prúdové spracovanie obrazu, bezstratovú kompresiu a hardvérovú i platformnú nezávislosť.

Obrázky formátu PNG môžu byť tak farebné (RGB), ako aj v tónoch sivej. Umožňujú uchovať až 48 bitov na jeden pixel pre farebné kanály a 16 bitov pre sivotónový kanál. Kompresia sa delí na dva stupne. V prvom kroku dochádza k filtrovaniu dát a tým k zvýšeniu efektívnosti kompresie. V druhom kroku sa dáta komprimujú algoritmom DEFLATE, ktorý je kombináciou algoritmu LZ77 a Hufmannovho kódovania. Tento proces je bezstratový, čo je kritické pre steganografické metódy v priestorovej doméne. Informácia uložená v pixeloch obrázka sa tak procesom kompresie nikde nestratí ani neznehodnotí.

JPEG

Joint Photographic Expert Group (JPEG) je najpoužívanejším spôsobom uchovávania obrazovej informácie. V skutočnosti sa jedná o metódu stratovej kompresie digitálnych obrázkov. Poskytuje nastaviteľnú úroveň kompresie a tým aj variabilný kompresný pomer a kvalitu výsledného obrázku. Používa sa v rôznych obrazových formátoch, medzi inými vo formátoch JFIF a EXIF. Práve prvý menovaný je najčastejšie považovaný za samotný JPEG a v tejto práci sú tieto názvy považované za ekvivalentné.

Formát JPEG/JFIF umožňuje uloženie sivotónových i farebných obrázkov. Využíva farebný model YCbCr a pre každý kanál má vyhradených 8 bitov. Disponuje tak 24-bitovou farebnou hĺbkou.

Hlavnou časťou metódy JPEG je kompresia pomocou diskrétnej kosínusovej transformácie (DCT). Táto operácia je stratová a spolieha sa na nedostatočné zrakové vnímanie ľudí. Z obrázka odstraňuje vysokofrekvenčné informácie, ktoré by ľudské oko nezachytilo. Samotná kompresia sa docieli vypustením nerelevantných informácií pomocou kvantizácie. Kvantifikované koeficienty DCT sú následne zapísané v sekvencii do výstupného súboru. Tieto koeficienty sú potom často využívané rôznymi steganografickými metódami.

3.3 LSB

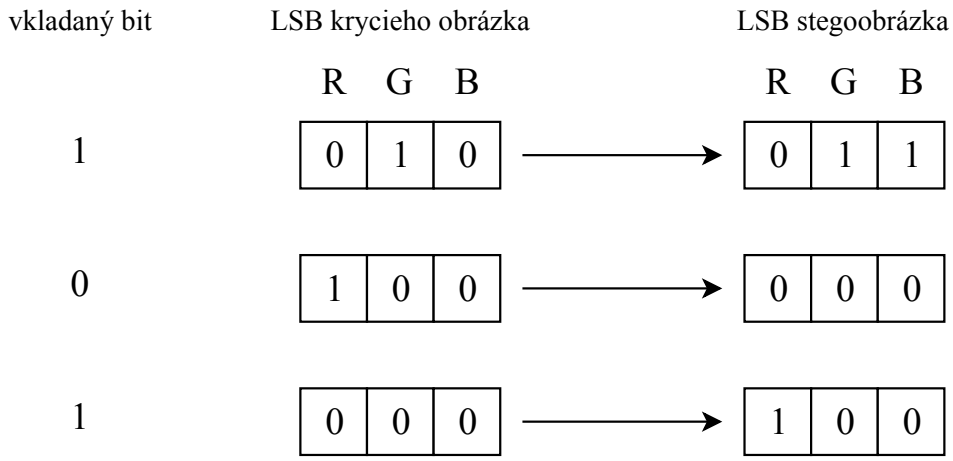
Najpoužívanejšou a najrozšírenejšou metódou v priestorovej doméne je metóda LSB (z angl. least significant bit). Už z jej názvu vyplýva podstata použitého princípu schovávania tajnej správy. Tajná správa je rozdelená na jednotlivé bity. Týmito bitmi tajnej správy sú nahradené najmenej významné bity hodnôt farebných kanálov alebo kanálu označujúceho intenzitu v prípade sivotónových obrázkov. Táto metóda je veľmi jednoducho implementovateľná a zmena intenzity farby o 1 stupeň je ľudskému oku nepostrehnuteľná. Je však ľahko odhaliteľná skúmaním vlastností stegoobrázka. LSB metóda sa totiž vyznačuje tým, že pixely s párnou hodnotou ponecháva, alebo zvýši o 1. S nepárnymi pixelmi pracuje opačne – buď ich ponechá nezmenené, alebo ich hodnotu o 1 zníži. To vytvára v histograme ľahko spozorovateľné dvojice susedných hodnôt.

3.4 Modifikovaná metóda LSB

Táto metóda [18] využíva princípy klasickej sekvenčnej metódy LSB, no na uloženie informácie nevyužíva všetky dostupné LSB. Základom modifikovanej metódy LSB je zvýšenie odolnosti voči analýze χ^2 testom a využíva najväčšiu slabinu tohto testu – náhodné roz-

loženie uloženej informácie. Pri náhodnom výbere pixelov, do ktorých sa uloží skrývaná informácia, musíme nejakým spôsobom oznámiť adresátovi správy, v ktorých pixeloch má informáciu hľadať. Jedným zo spôsobov môže byť dohoda na kľúči, podľa ktorého sa budú dané bity vyberať. Táto forma vyžaduje určitú komunikáciu medzi dvomi stranami, ktorá však môže byť odpozorovaná. To je nežiaduce, keďže podstatou steganografie je zatajenie samotného faktu, že medzi dvoma subjektmi existuje akákoľvek komunikácia. Farebné obrázky však ponúkajú možnosť ako problém s rozposlaním kľúča obísť. Ak je obrázok vo farebnej palete typu RGB, dá sa jeden z kanálov využiť ako kľúč, podľa ktorého sa informácia bude ukladať.

Modifikovaná metóda LSB využíva zelený kanál ako pomocnú informáciu, podľa ktorej sa rozhoduje o výbere kanála na uloženie skrývaných bitov. Na obrázku 3.1 je ilustratívne naznačený proces vkladania informácie do obrázka. V obrázku sú zaznačené najmenej významné bity jednotlivých pixelov rozdelených po farebných kanáloch.



Obr. 3.1: Proces vkladania skrytej informácie v modifikovanej LSB metóde.

V prípade, že je hodnota LSB zeleného kanála párna, vkladá sa bit do LSB červeného kanála daného pixla. Ak je nepárna, vyberie sa kanál modrý. Rozloženie hodnôt LSB zeleného kanála zabezpečuje pseudonáhodnosť modifikácie bitov v ostatných kanáloch. Táto skutočnosť znemožňuje odhalenie skrytej informácie za pomoci χ^2 testu, keďže informácia nie je uložená v súvislých blokoch od začiatku obrázka.

3.5 ±1 vkladanie

Metóda ±1 vkladania [3] (tiež známa ako LSB matching) je sofistikovanejšou verziou LSB. Hlavný rozdiel oproti metódam LSB je v tom, že v prípade nezhody najmenej významného bitu pixla a vkladaného bitu nedochádza len k priamemu nahradeniu tohto bitu. Namiesto toho sa hodnota pixla náhodne zvýši alebo zníži o 1. V ideálnom prípade by zvýšenie a zníženie hodnoty mali mať uniformné rozloženie – takto sa zabráni efektu, ktorý vnáša do histogramu metóda LSB. Nevznikajú tak páry susedných hodnôt v histograme obrázka a stegoobrázok tak nie je náchylný na útok pomocou χ^2 testu. Zároveň je správa v stegoobrázku čitateľná rovnako ako správa vložená pomocou LSB. Najmenej významné bity majú totiž v prípade uloženia rovnakej správy oboma metódami rovnaké hodnoty, no hodnoty pixelov sa líšia.

Metóda ±1 vkladania môže byť vyjadrená nasledovne:

$$p_s(i,j) = \begin{cases} p_c(i,j)+1 & \text{ak } b \neq LSB(p_c(i,j)) \text{ a } (k>0 \text{ alebo } p_c(i,j)=0), \\ p_c(i,j)-1 & \text{ak } b \neq LSB(p_c(i,j)) \text{ a } (k<0 \text{ alebo } p_c(i,j)=255), \\ p_c(i,j) & \text{ak } b = LSB(p_c(i,j)), \end{cases}$$

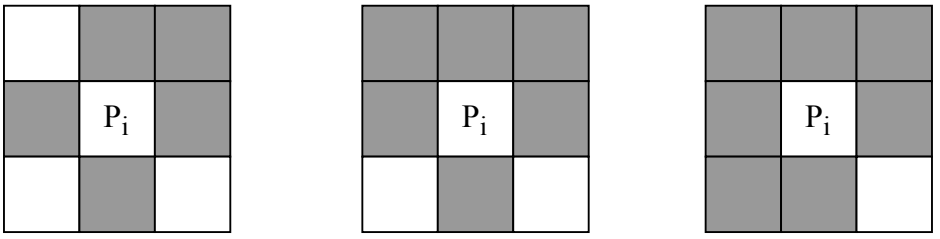
kde $p_s(i,j)$ a $p_c(i,j)$ sú hodnoty pixla stegoobrázka, resp. krycieho obrázka, na pozícii i,j, k je náhodná veličina s rovnomerným rozdelením z množiny $\{-1,1\}$, LSB je funkcia vracajúca najmenej významný bit pixla a b prezentuje hodnotu vkladaného bitu.

Ani metóda ±1 vkladania však nie je odolná voči štatistickým stegoanalytickým metódam. Princíp jej prelomenia je popísaný v podkapitole 4.3.

3.6 Metóda susedov

Metóda susedov je adaptívnou obrazovou steganografickou metódou [16]. Jej podstatou je ukrytie variabilného množstva informácie do jednotlivých pixelov, vzhľadom na jeho okolie. Vysoké množstvo vloženej informácie totiž vo všeobecnosti môže badateľne zmeniť pôvodný pixel. V častiach obrazu, ktoré sú súvislé, by takáto zmena bola ľahko postrehnuteľná ľudským okom. Táto metóda hľadá v krycom obraze miesta, ktoré sa vyznačujú vysokou členitosťou (napríklad okraj hrán). V týchto miestach potom ukladá zvýšené množstvo informácie v porovnaní s miestami, ktoré sú súvislé.

Členitosť okolia pixla, do ktorého sa uloží skrývaná informácia, záleží na rozdieloch hodnôt okolitých pixelov. Použité pixely na určenie množstva vloženej informácie sú zobrazené na obrázku 3.2. Využíva sa 5 až 8 okolitých pixelov podľa výberu osoby využívajúcej túto metódu.



Obr. 3.2: Pixely použité na určenie počtu bitov tajnej správy v metóde susedov.

Množstvo bitov vkladanej informácie záleží na rozdiele d pixelov s najvyššou a najnižšou hodnotou, nachádzajúcich sa v špecifikovanom okolí:

$$d = p_{max} - p_{min},$$

kde p_{max} označuje maximálnu hodnotu a p_{min} minimálnu hodnotu. Z tohto rozdielu sa získa počet ukrývaných bitov

$$n = \begin{cases} 1 & \text{ak } d \leq 1, \\ \log_2 d & \text{inak.} \end{cases}$$

V prípade, že n je väčšie ako 4, nastaví sa počet vkladaných bitov na 4. Vyššia hodnota by totiž mala za následok rapídne zníženie kvality stegoobrázka a jednoduché odhalenie

vloženej informácie voľným okom. Nová hodnota pixla je potom

$$p_n = p - p \bmod 2^n + b,$$

kde b predstavuje číslo vytvorené z n bitov bitovej postupnosti skrývanej informácie. Táto hodnota sa upraví v dvoch prípadoch:

1. Ak $2^{n-1} < p_n - p < 2^n$ a $2^n \leq p_n$, potom $p_n = p_n - 2^n$.
2. Ak $-2^n < p_n - p < -2^{n-1}$ a $p_n < 256 - 2^n$, potom $p_n = p_n + 2^n$.

Pri dekódovaní správy zo stegoobrázka sa postupuje pri počítaní počtu n uložených bitov rovnakým spôsobom. Uloženú hodnotu potom získame ako

$$b = p \bmod 2^n,$$

a číslo b rozložené na n bitov potom predstavuje bity uloženej tajnej správy.

Táto metóda sa od ostatných steganografických metód spomenutých v kapitole 3 odlišuje tým, že ako jediná zasahuje aj do iných ako najmenej významných bitov jednotlivých pixelov. Pre potreby tejto práce bola zvolená preto, aby sme poukázali na nedostatky štatistických stegoanalytických metód v kapitole 4. Tieto metódy sú zamerané na odhaľovanie LSB steganografie. Vzhľadom na fakt, že metóda susedov nie je typickým zástupcom LSB steganografie, LSB stegoanalýza by mala pri jej odhaľovaní zlyhať. Výsledky stegoanalytických metód popísaných v kapitole 4 pri odhaľovaní steganografickej metódy susedov sa nachádzajú v podkapitole 4.4.

3.7 Porovnanie steganografických metód v priestorovej doméne

Závery vyplývajúce z tejto podkapitoly boli výsledkom experimentov autora práce.

Nedetekovateľnosť
Všetky implementované metódy ovplyvňujú výsledný stegoobrázok v miere, ktorú nie je možné postrehnúť ľudským okom. Za prepdokladu, že krycie obrázky pozostávajú z pixelov, ktoré majú aspoň 8 bitov, rozlišovacia schopnosť ľudského zraku nie je dostatočná na to, aby zistila vytvorené zmeny v krycom obrázku. Odolnosť voči odhaleniu stegoanalytickými metódami je však naprieč jednotlivými steganografickými metódami rôzna. Všeobecne platí, že výkon steganografických metód klesá s množstvom šumu, ktorý sa nachádza v krycom obrázku. Všetky metódy popísané v kapitole 4 totiž určitým spôsobom hľadajú novovzniknutý šum, ktorý bol do krycieho obrázka zanesený steganografiou.

Z experimentov však vyplýva, že najodolnejšou metódou je metóda ±1 vkladania. Tá bola totiž navrhnutá tak, aby ju nebolo možné odhaliť χ^2 testom a v jej odhaľovaní zlyháva aj RS analýza. Pri vhodnom výbere krycieho obrázka sa dokonca ani špecializovanej metóde s využitím HCF COM detektora nedarí určiť, či je obrázok krycí alebo stegoobrázok.

Najmenej odolnou metódou je najjednoduchšia sekvenčná LSB metóda. S vysokou presnosťou sa ju podarilo odhaliť za pomoci všetkých implementovaných stegoanalytických metód. Najvyššiu úspešnosť a presnosť v tomto prípade dosahovala metóda χ^2 testu.

Kapacita
Vlastnosť, v ktorej sa jednotlivé steganografické metódy líšili najviac, je kapacita. Tá určuje, koľko percent krycieho obrázka môže byť využitých na ukrytie informácie.

Najvyššiu kapacitu prakticky dosahujú zhodne metódy ±1 vkladanie a sekvenčná LSB metóda. Obe metódy dokážu využiť všetky pixely krycieho obrázka a v prípade, že obrázok je farebný, dokážu využiť všetky farebné kanály bez toho, aby zaniesli do obrázka zmeny viditeľné ľudským okom. Presne tretinovú kapacitu oproti týmto metódam má modifikovaná LSB metóda. Tá totiž dokáže využiť iba jeden farebný kanál každého pixla. Ďalším obmedzením tejto metódy je, že môže byť aplikovaná iba na farebné krycie obrázky.

Metóda susedov je špeciálny prípad. Teoretické hodnoty množstva bitov ukrývanej informácie tejto metódy sa totiž dramaticky menia v závislosti na krycom obrázku. Najnižšia hodnota, ktorú môžeme za pomoci metódy susedov uložiť je približne 1/4 počtu pixelov krycieho obrázka. Takáto situácia nastáva v prípade, že vkladáme do pixelov iba 1 bit informácie. Keďže na vkladanie sa používa každý druhý pixel v každom druhom riadku, použitých pixelov je približne 1/4. V prípade, že do každého pixelu vložíme maximálne povolené množstvo (v našom prípade 4 bity), dosahuje táto metóda takmer kapacitu sekvenčnej LSB metódy. Počet bitov uložených do jednotlivých pixelov je v testovanej sade 90 sivotónových obrázkov 2,78 bitu na využiteľný pixel v prípade využitia okolia 5 pixelov. V tabuľke 3.1 sa nachádzajú priemerné hodnoty kapacity metódy susedov podľa veľkosti skúmaného okolia. Presný počet využiteľných pixelov v krycom obrázku s rozmermi n a m je

$$\lfloor (n-1)/2 \rfloor \cdot \lfloor (m-1)/2 \rfloor.$$

	priemerná kapacita	pomer voči LSB	bity na pixel
5 susedov	33658	0,68	2,78
6 susedov	34595	0,70	2,85
7 susedov	35118	0,71	2,90
8 susedov	35542	0,72	2,94

Tabuľka 3.1: Kapacita metódy susedov s ohľadom na veľkosť okolia pixelov.

Robustnosť a odolnosť voči manipulácii
Všetky steganografické metódy v priestorovej doméne predstavené v tejto kapitole sú rovnako náchylné na zásahy do stegoobrázka. Jedinou úpravou, ktorá nepoškodí uloženú informáciu je otočenie stegoobrázka. Vtedy je však nutné zmeniť smer, ktorým sa prechádza stegoobrázok pri čítaní ukrytej informácie. Akákoľvek operácia, ktorá mení hodnoty pixelov aplikovaná na celý stegoobrázok, má však za následok úplnú stratu ukrytej operácie. Podobný efekt má prevod stegoobrázkov do formátu, ktorý využíva stratovú kompresiu (napr. JPEG). Manipulácie len s malými časťami obrázkov majú najhorší efekt na informáciu zakódovanú pomocou metódy susedov. Na úplnú stratu informácie stačí zmena jediného pixla, ktorý rozhoduje o počte bitov uložených v susednom pixeli. To môže mať za následok pridanie alebo vynechanie bitov z bitovej postupnosti skrytej informácie. Posun čo i len o jednu pozíciu znehodnotí obsah natoľko, že nie je možné bitovú postupnosť správne interpretovať.

Zmena hodnôt pixelov v určitej časti stegoobrázka vytvoreného pomocou ostatných metód má za následok znehodnotenia iba tej časti informácie, ktorá sa nachádza v zmenených pixeloch. Keďže každý pixel nesie práve 1 bit informácie, nedochádza k žiadnym posunom

výslednej bitovej postupnosti a časti informácie nachádzajúce sa v nezmenených oblastiach obrázka sa dajú prečítať.

Ani jedna z metód nie je odolná voči orezaniu obrázka. Táto operácia má totiž na výslednú bitovú postupnosť rovnaký efekt ako zmena hodnoty pixla v prípade metódy susedov – posunutie bitovej postupnosti zakódovanej správy.

3.8 Prehľad metód vo frekvenčnej doméne

Pre doplnenie prehľadu metód obrazovej steganografie, sú v tejto časti uvedené metódy, ktoré na uloženie skrývanej informácie využívajú frekvenčnú doménu obrázkov. Vďaka tomu sú schopné pracovať s formátmi podporujúcimi stratovú kompresiu dát. Jedným z takýchto formátov je JPEG. Vzhľadom na rozsah použitia obrázkov tohoto formátu (bežne používaný formát uloženia fotografií) je nutné mať k dispozícii metódy schopné pracovať s týmito obrázkami.

Uloženie bitu informácie do samotných pixelov je v tomto formáte neefektívne – dôvodom je totiž zmena či strata informácie po aplikovaní stratovej kompresie. Nasledujúce metódy predstavujú riešenie tohoto problému pomocou využitia frekvenčnej domény obrázkov formátu JPEG.

3.8.1 JSteg

Metóda JSteg bola jednou z prvých metód, ktoré využívali na ukrytie tajnej správy JPEG obrázky. Princípom tejto metódy je ukrytie jedného bitu tajnej správy do viacerých bitov krycieho obrázka, čím sa zníži veľkosť zmeny zanesenej do krycieho obrázka. Rozprestrenie tejto zmeny je dosiahnuté pozmenením koeficientov DCT, využívaných pri vytváraní JPEG obrázka. Zmena koeficientov prebieha pomocou LSB princípu známeho z metód v priestorovej doméne. Jednotlivé koeficienty ovplyvňujú plochu 8×8 pixelov, a tak je bit tajnej správy uložený vo viacerých pixeloch stegoobrázka. Algoritmus JSteg nevyužíva koeficienty s hodnotou 0 a 1, keďže zmena týchto koeficientov by ovplyvnila stegoobraz natoľko, že by bol odhaliteľný ľudským okom. Problémom je však fakt, že kvantifikované DCT koeficienty majú z veľkej časti hodnoty 0 a 1, čo razantne znižuje kapacitu metódy JSteg. Z tohto dôvodu bola navrhnutá nová kvantizačná tabuľka, ktorá zachováva kvalitu JPEG obrázka a zároveň zvyšuje kapacitu algoritmov využívajúcich JPEG ako krycí obrázok [4].

Metóda JSteg je zraniteľná útokom pomocou χ^2 testu. Vzhľadom na fakt, že pracuje vo frekvenčnej doméne prakticky rovnako ako metóda LSB 3.3 v priestorovej doméne, trpí rovnakým neduhom – modifikáciou histogramu predvídateľným spôsobom. Pri skúmaní steganografickej modifikácie sa však analýza nezameriava priamo na histogram výsledného obrázka, ale využíva vlastnosti histogramu koeficientov DCT použitých na vytvorenie stegoobrázka. Po zostavení histogramu koeficientov DCT sú v prípade stegoobrázkov znateľné susedné páry hodnôt, ktoré potom vedú k odhaleniu steganografickej manipulácie s obrázkom χ^2 testom 4.1.

3.8.2 OutGuess

Metóda OutGuess je vylepšením metódy JSteg. Jej snahou je odstrániť zraniteľnosť JSteg-u, ktorou je odhaliteľnosť pomocou χ^2 metódy. Vynájdený bol práve z dôvodu prelomenia algoritmu JSteg pomocou χ^2 testu.

Algoritmus metódy OutGuess pracuje v dvoch krokoch. Prvým je ukrytie informácie v kvantifikovaných koeficientoch spôsobom, ktorý využíva metóda JSteg – pomocou metódy LSB. Druhý krok následne zaručí to, že histogram všetkých koeficientov stegoobrázka je rovnaký ako histogram krycieho obrázka. Vzhľadom na fakt, že je histogram koeficientov stegoobrázka nezmenený, χ^2 test stegoobrázka musí dosiahnuť rovnaký výsledok ako v prípade obrázka krycieho.

Kapitola 4

Metódy obrazovej stegoanalýzy

Všetky steganografické metódy trpia svojimi vlastnými chybami, ktoré sú kvôli podstate daných metód jednoducho neodstrániteľné. Vývoj spôsobov a metód, ktoré sú schopné odhaliť steganografickú manipuláciu s krycími obrázkami, je tak logický. Dôvodov je viacero – odhaľovanie informácií, ktoré majú byť utajené, alebo hodnotenie výkonu či bezpečnosti týchto metód sú najvýznamnejšie katalyzátory vzniku stegoanalytických metód. V tejto kapitole budú priblížené tri špecificky zamerané štatistické stegoanalytické metódy, využívajúce slabiny steganografických metód zaoberajúcich sa steganografiou v priestorovej doméne.

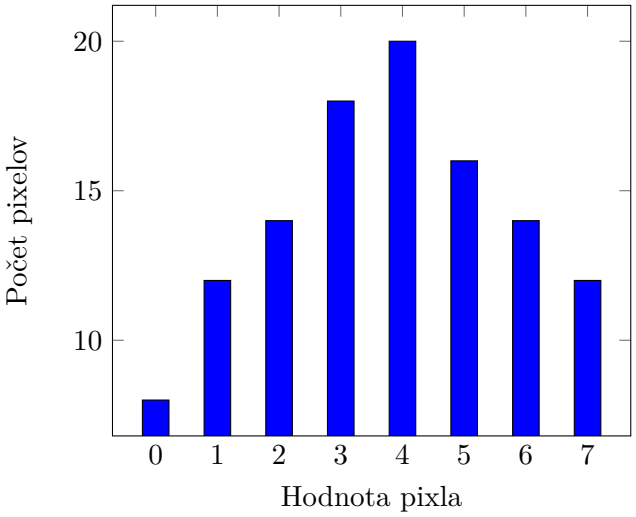
4.1 χ^2 test

Autori tejto metódy ukazujú, ako sa dá využiť na odhalenie nielen samotnej prítomnosti steganografickej informácie v potenciálnom stegoobrázku, ale aj na určenie dĺžky skrytej správy [17]. Zároveň poukazujú na fakt, že táto metóda je úspešná pri odhaľovaní sekvenčnej LSB steganografie nielen v priestorovej, ale aj vo frekvenčnej doméne, ktorú využívajú obrázky formátu JPEG.

4.1.1 Popis metódy

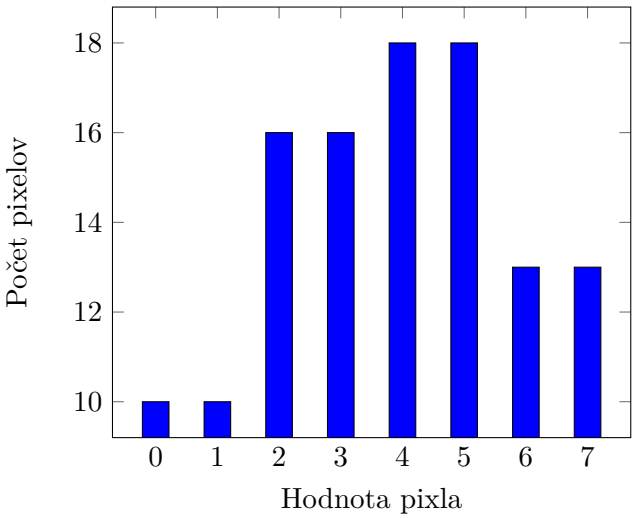
Najpoužívanejším štatistickým nástrojom, ktorý popisuje ľubovoľný obrázok a hlavne rozdelenie intenzít farieb, ktoré sa v ňom nachádzajú, je histogram. Histogram vyjadruje početnosť jednotlivých hodnôt intenzít, ktoré môžu naberať pixeli v obrázku. Na obrázku 4.1 sa nachádza príklad obrázku obsahujúceho pixely intenzít v rozsahu 0 až 7. Neopatrná modifikácia krycieho obrázka môže mať za následok zmeny v stegoobrázku, ktoré sú buď viditeľné voľným okom, alebo sa premietnu do iných vlastností stegoobrázka – najčastejšie práve do histogramu. Najjednoduchšia steganografická metóda LSB 3.3 síce nemení hodnoty intenzít pixelov natoľko, aby ich ľudské oko postrehlo, no modifikuje obrázok presne definovaným spôsobom.

Z kapitoly 3.3 vieme, že metóda LSB mení najnižšie bity pixelov obrázka podľa toho, aký bit informácie potrebuje do krycieho obrázka uložiť. Pri tomto procese teda vie zmeniť párne čísla na vyššie nepárne a naopak, nepárne čísla na nižšie párne. Keďže metóda LSB nezasahuje do žiadnych iných bitov okrem toho najmenej významného, nemôže znížiť hodnotu párneho čísla ani zvýšiť hodnotu nepárneho. Táto vlastnosť zmeny najnižšieho bitu vytvára v histograme dvojice susedných hodnôt – nižšia párna a hneď nasledujúca nepárna. Celkový počet pixelov s hodnotami v rámci tejto dvojice je nemenný aj po zásahu do LSB



Obr. 4.1: Teoretický histogram krycieho obrázka.

krycieho obrázka. Pri uniformnom rozložení prepisovaných bitov v obrázku sa však hodnoty v rámci takýchto dvojíc vyrovnávajú (obr. 4.2).



Obr. 4.2: Histogram obrázka po modifikácii metódou LSB.

Podstatou metódy χ^2 testu je porovnanie sledovanej vzájomnej frekvencie medzi prvkami týchto dvojíc a očakávanej frekvencie, ktorá by mala byť v obrázku pozorovaná za predpokladu, že je stegoobrázkom.

Nájdenie očakávanej frekvencie výskytu hodnôt pre jednotlivé dvojice je najdôležitejšou časťou útoku. Počas útoku analýza nemá k dispozícii pôvodný krycí obrázok, resp. nevie, či ním nie je práve testovaný obrázok, a nemôže tak z krycieho obrázka vydedukovať očakávanú frekvenciu susedných hodnôt histogramu. Čo však vieme je, že metóda LSB nemení súčet frekvencií susedných hodnôt. Očakávanou frekvenciou v prípade stegoobrázka by tak mal byť aritmetický priemer frekvencií susedných hodnôt v histograme. Postup tejto metódy je teda nasledovný:

1. Predpokladáme k kategórií a náhodnú vzorku pozorovaní. Každé pozorovanie spadá do jednej z kategórií, avšak zameriavame sa iba na polovicu z nich, konkrétne na párne hodnoty, ktoré reprezentujú pozorované hodnoty. Počet kategórií dosahuje teda maximálne polovicu dĺžky histogramu. Ďalej sa počet kategórií znižuje o 1 v každom z prípadov, keď pozorované dve po sebe idúce hodnoty histogramu nedosahujú súčet 5 – tieto hodnoty nebudeme uvažovať.

2. Očakávaná hodnota pozorovania i je vypočítaná z dvoch po sebe idúcich hodnôt histogramu nasledovne:
$$n_i^{exp} = \frac{h(2i) + h(2i+1)}{2},$$
kde $h(k)$ predstavuje histogram testovaného obrázka.

3. Za pozorovanú hodnotu v kategórii i určíme i-tú párnu hodnotu histogramu:
$$n_i = h(2i).$$

4. Z pozorovaných a očakávaných frekvencií potom vypočítame hodnotu χ^2 s $k-1$ stupňami voľnosti, kde k predstavuje počet uvažovaných kategórii z bodu 1:
$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(n_i - n_i^{exp})^2}{n_i^{exp}}.$$

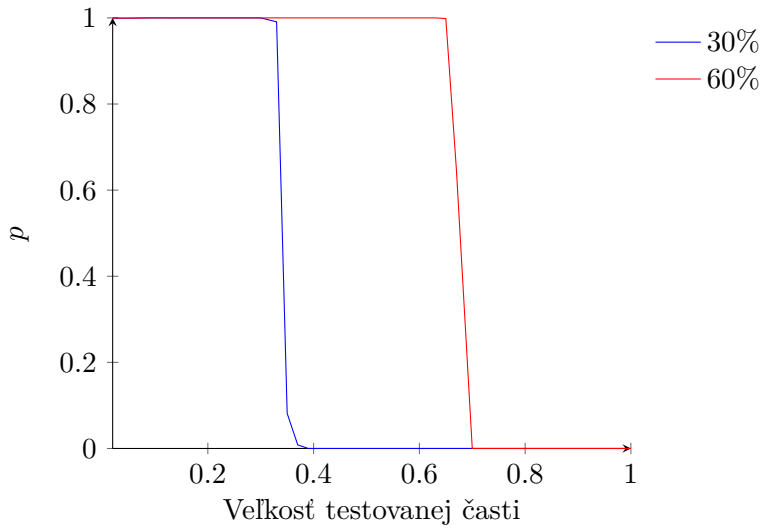
5. Posledným krokom je vypočítanie pravdepodobnosti p určujúcej správnosť hypotézy, že testovaný obrázok je stegoobrázok. Pravdepodobnosť p hovorí nakoľko je pravdepodobné, že n a n_{exp} sú závislé, resp. ako veľmi sú si podobné:
$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})} \int_0^{\chi^2_{k-1}} \mathrm{e}^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} \mathrm{d}x.$$

Na to, aby bola prítomnosť správy odhalená, musia si n a n_{exp} byť čo najviac podobné. To znamená, že čo najviac najmenej významných bitov musí byť pozmenených. To nastáva iba v prípade, že sa tajná správa nachádza v celom testovanom obrázku. Aby mohla byť odhalená aj kratšia správa, resp. aby metóda dokázala určiť dĺžku danej správy, je nutné tento algoritmus vykonávať nad časťami obrázku.

Metóda zvláda označiť iba stegoobrázky, ktorých kapacita bola využitá takmer naplno. Na odhalenie kratších správ vytvoríme obrázky z testovaného tak, aby v nich bola správa zakódovaná s využitím ich plnej kapacity. Postupne budeme sekvenčne zvyšovať počet pixelov nového obrázka od 0 a každý takýto obrázok podrobíme χ^2 testu. V momente, keď pravdepodobnosť výskytu správy v celom novom obrázku klesne pod určitú hranicu, určíme predchádzajúci obrázok ako ten, ktorý v celom svojom obsahu skrýval zakódovanú správu. Na obrázku 4.3 je zobrazená hodnota p pre jednotlivé novovytvorené obrázky. Veľkosť obrázka v momente, v ktorom prudko klesne hodnota p, určuje zároveň aj veľkosť skrytej správy. V tomto konkrétnom prípade bola kapacita obrázka využitá na 30% a 60%.

4.1.2 Experimentálne výsledky

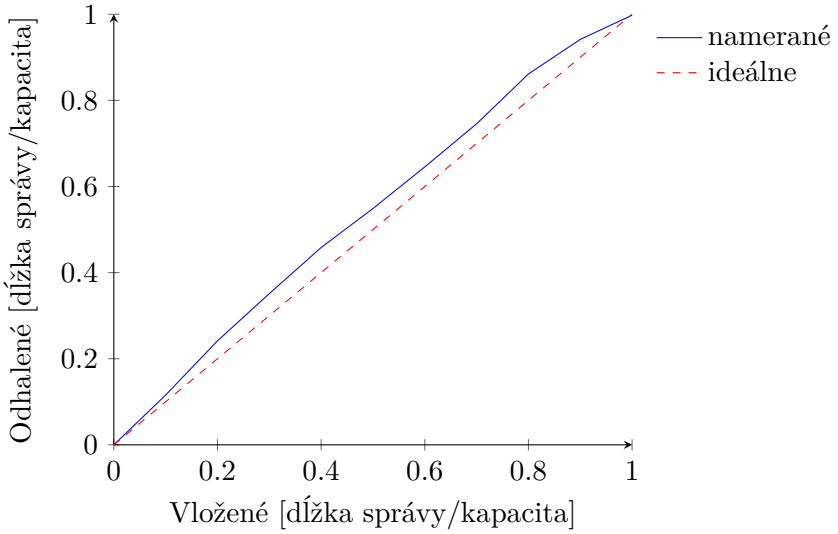
Experimenty prebiehali so sadou čiernobielych obrázkov formátu PNG. Počet testovaných obrázkov dosiahol 200. Jednotlivé krycie obrázky boli vytvorené prevedením do odtieňov



Obr. 4.3: Pravdepodobnosť p, vypočítaná z časti testovaného obrázka.

sivej a zmenšením fotografií vytvorených mobilným telefónom LG Nexus 5X. Z každého krycieho obrázka bol neskôr vytvorený stegoobrázok obsahujúci skrytú správu s dĺžkou postupne 10-100% svojej kapacity. Tento proces prebiehal po 10% inkrementoch. Zvolenou steganografickou metódou bola sekvenčná LSB metóda 3.3. Napokon boli všetky takto vytvorené stegoobrázky podrobené χ^2 testu.

Pomer množstva odhalenej správy k množstvu ukrytej správy pomocou sekvenčnej LSB metódy sa nachádza na obrázku 4.4.



Obr. 4.4: Odhadovaná veľkosť správy ukrytej metódou LSB pomocou χ^2 testu.

Pre overenie predpokladu, že metóda χ^2 testu zlyháva pri akejkoľvek inej ako sekvenčnej LSB steganografii, bola vykonaná analýza stegoobrázkov vytvorených pomocou modifikovanej LSB metódy i pomocou ± 1 vkladania. V prvom prípade sa testovali farebné obrázky formátu PNG, v ktorých bola využitá plná kapacita obrázka. Test prebiehal postupne po

jednotlivých kanáloch farebného obrázka a pre každý kanál bola stanovená dĺžka správy, ktorú podľa χ^2 testu ukrýva. Priemerná dĺžka správy sa odchyľovala o 0,5% od údajov, ktoré boli získane analýzou krycích obrázkov – teda aj tieto stegoobrázky boli chybne označené ako krycie obrázky.

V druhom prípade prebiehal test čiernobielych obrázkov formátu PNG, do ktorých bola vložená informácia pomocou metódy ±1 vkladania. Predpoklad bol, že analýza takýchto obrázkov neodhalí žiadnu steganografickú manipuláciu, resp. žiadnu vloženú informáciu, keďže podstatou ±1 vkladania je predísť odhaleniu skúmaním histogramu

Úprava výpočtu χ^2
Výpočet χ^2 a p predstavený v 4.1.1 neposkytoval pôvodne žiadne výsledky. Pri využití funkcie `chisquare` z knižnice SciPy sa nepodarilo získať pravdepodobnosti, ktoré by viedli k výsledkom dosiahnutým autormi metódy [17]. Táto funkcia poskytuje výpočet tzv. testu nezávislosti, ale pre potreby tejto metódy je nutný tzv. *goodness of fit* test. Metóda výpočtu χ^2 je teda pozmenená nasledovne:

$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(n_i - r \cdot n_i^{exp})^2}{r \cdot n_i^{exp}},$$

kde r získame ako

$$r = \frac{\sum_{f_o \in n} f_o}{\sum_{f_e \in n_{exp}} f_e}.$$

4.2 RS analýza

Množstvo steganografických metód pracujúcich s LSB kvôli zvyšovaniu neodhaliteľnosti skrytej informácie nepracuje sekvenčne. Aj najjednoduchšie metódy ako LSB, ktorá je opísaná v kapitole 3.3, môžu byť ľahko modifikované spôsobom, ktorý znemožňuje použitie χ^2 testu, resp. tento test pri skúmaní stegoobrázkov vytvorených takýmito metódami zlyháva. Príkladom môže byť náhodný výber bitov, do ktorých sa skrývaná informácia ukladá. Tento prístup využíva modifikovaná metóda LSB spomenutá v 3.4. Na odhalenie takýchto metód je teda nutný iný postup ako χ^2 test. Jednou z metód, ktorá je schopná odhaliť nesekvenčnú steganografickú manipuláciu s obrázkom, je RS analýza [8].

4.2.1 Popis metódy

Podstatou metódy s názvom RS analýza je porovnávanie počtu skupín pixelov s určitými vlastnosťami pred špecifickou manipuláciou s potenciálnym stegoobrázkom a po nej. Pre plné pochopenie tejto metódy je nutné vysvetlenie teoretických základov a vlastností skúmaných skupín pixelov.

Majme obrázok (pre zjednodušenie vysvetlenia v odtieňoch sivej) zložený z pixelov, ktoré naberajú hodnoty $0, \ldots, N-1$ pre N bitov, ktoré kódujú jeden pixel. Tieto pixely rozdelíme do disjunktných skupín o početnosti n. Tvar týchto skupín môže byť rôzny, podstatnou vlastnosťou je, aby tieto pixely boli susedné. V prípade tejto práce boli použité skupiny štvorcového tvaru s veľkosťou $n = 4$, teda skupiny 2×2 pixelov. Možnou alternatívou je aj skupina tvaru 1×4, ktorú použili autori tejto metódy v [8]. Definujeme diskriminačnú funkciu $f(x_1, x_2, \ldots, x_n) \in \mathbb{R}$, ktorej úlohou je zachytiť, v akej miere sa pixely v danej skupine od seba odlišujú svojou hodnotou. Funkcia f teda popisuje členitosť určitej

časti obrázka – v našom prípade časti o veľkosti 4 pixelov. Čím vyššiu hodnotu dosiahne diskriminačná funkcia, tým členitejšia je skupina pixelov $G = (x_1, \ldots, x_n)$. Najčastejším variantom diskriminačnej funkcie je suma absolútnych hodnôt rozdielov susedných pixelov. Pre potreby tejto práce má funkcia f tvar

$$f(x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}) = \sum_{i=1}^{2} |x_{i,1} - x_{i,2}| + |x_{1,i} - x_{2,i}|.$$

Vyššie spomenutou špecifickou manipuláciou je tzv. prevracanie hodnôt pixelov (z angl. flipping). Predstavuje ju invertibilná funkcia F, platí pre ňu teda vzťah $F(F(x)) = x$. Vytvoríme tri varianty tejto funkcie. Prvým variantom F_1 je zámena LSB argumentu tejto funkcie. Funkcia F_1 má teda tvar

$$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255.$$

Druhý variant predstavuje funkcia F_{-1}, ktorá vykonáva zámenu LSB posunutého argumentu – $F_{-1}(x) = F_1(x + 1) - 1$. Funkcia F_{-1} [1] teda vyzerá takto:

$$F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256.$$

Posledným variantom je funkcia $F_0(x) = x$. Na základe aplikácie *flipping* funkcie a diskriminačnej funkcie môžeme rozdeliť skupiny pixelov do troch rôznych skupín:

- regulárne $G \in R \Leftrightarrow f(F(x_1), \ldots, F(x_n)) > f(x_1, \ldots, x_n)$,
- singulárne $G \in S \Leftrightarrow f(F(x_1), \ldots, F(x_n)) > f(x_1, \ldots, x_n)$,
- nepoužiteľné $G \in U \Leftrightarrow f(F(x_1), \ldots, F(x_n)) > f(x_1, \ldots, x_n)$.

Každému pixelu zo skupiny G však môže byť priradený iný variant funkcie F. Voľba tohto variantu F je určená maskou $M = (m_1, \ldots, m_n), m \in \{-1, 0, 1\}$. Hodnota m_i určuje index variantu funkcie F použitej na zmenu hodnoty pixla x_i. Funkcia F slúži na malú a návratnú zmenu hodnoty pixelov. Pomocou tejto zmeny zavádzame do testovaného obrázka šum, pomocou ktorého vieme odhaliť prítomnosť existujúceho steganografického šumu. Takáto zmena pixelov v krycích obrázkoch vedie k zvýšeniu hodnoty diskriminačnej funkcie aplikovanej na skupiny pixelov a potom vedie k zvýšeniu počtu regulárnych skupín.

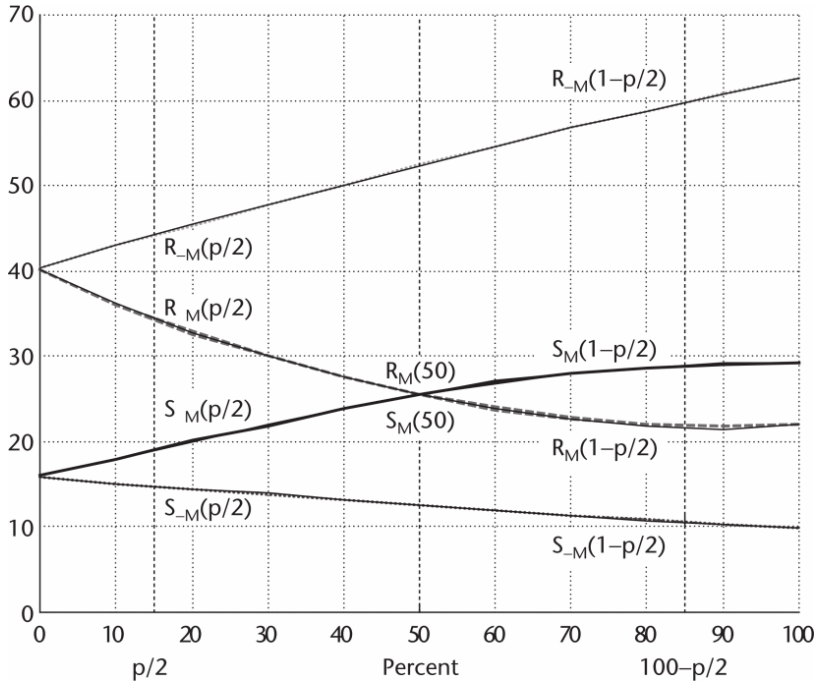
Za pomoci masky M a vyššie spomenutých funkcií získavame z obrázka počty regulárnych a singulárnych skupín R_M, resp. S_M, ktoré vyjadrujú pomer počtu daných skupín k celkovému počtu všetkých skupín pixelov. Podobne pre invertovanú masku $-M$ stanovíme počty skupín R_{-M} a S_{-M}. Z rozdelenia skupín pomocou diskriminačnej funkcie platí, že $R_M + S_M \leq 1$ a $R_{-M} + S_{-M} \leq 1$. Autori tejto metódy predpokladajú, že počty regulárnych a singulárnych skupín by sa nemali výrazne zmeniť so zmenou masky za invertovanú masku, a teda, že platí

$$R_M \approx R_{-M}, S_M \approx S_{-M}. \tag{4.1}$$

Toto tvrdenie je aj podložené testovaním krycích obrázkov z rôznych zdrojov. Rovnosť počtu skupín sa však ruší v prípade zmeny LSB jednotlivých pixelov. Čím viac pixelov je ovplyvnených steganografickou manipuláciou, tým väčší rozdiel je možné medzi korešpondujúcimi skupinami sledovať. Zároveň sa rozdiel $R_M - S_M$ znižuje, až dosiahne 0 v prípade, že dĺžka

[1] Pri implementácii je potrebné použiť dostatočne veľké typy premenných, keďže táto funkcia pracuje v bitovom rozsahu o 1 väčšom ako je bitový rozsah pixelov.

vloženej správy dosiahne polovicu kapacity krycieho obrázka (čo znamená, že polovica pixelov bola ovplyvnená steganografickým šumom). Vkladanie informácie do krycieho obrázka má ale opačný efekt na rozdiel $R_{-M} - S_{-M}$. Čím dlhšia správa je do krycieho obrázka vložená, tým vyššia je hodnota rozdielu týchto dvoch skupín. Na obrázku 4.5 sú znázornené počty skupín ako funkcie dĺžky skrytej správy.



Obr. 4.5: Počty regulárnych a singulárnych skupín na základe dĺžky správy [8].

Podstatou tejto stegoanalytickej metódy je odhadnutie tvaru kriviek z obrázka 4.5 a výpočet ich vzájomných priesečníkov. Autori metódy pomocou experimentov zistili, že funkcie R_{-M} a S_{-M} predstavujú priamky, zatiaľ čo zvyšné funkcie R_M a S_M môžu byť aproximované polynomiálnou funkciou druhého radu.

Na to, aby sme mohli aproximovať všetky štyri funkcie, potrebujeme pre dané funkcie dva až tri body, vzhľadom na fakt, že dve funkcie sú druhého radu. Za predpokladu, že testovaný potenciálny stegoobrázok obsahuje skrytú správu s dĺžkou p (v percentách kapacity obrázka), vypočítame hodnoty funkcií v bode $p/2$ – $R_M(p/2)$, $S_M(p/2)$, $R_{-M}(p/2)$ a $S_{-M}(p/2)$. Vzhľadom na predpoklad, že správa je náhodná postupnosť bitov, k zámene bitov dochádza iba v polovici prípadov. Hodnoty $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$, $S_{-M}(1-p/2)$ dostaneme prevrátením hodnôt všetkých pixelov pomocou funkcie F_1 a spočítaním jednotlivých regulárnych a singulárnych skupín po aplikácii oboch masiek.

Posledné body, ktoré nám ostávajú, sú body $R_M(1/2)$ a $S_M(1/2)$. Jednou možnosťou je získanie týchto hodnôt opakovaným vložením náhodnej správy do polovice pixelov a vypočítaním počtu skupín z týchto vzoriek, čo je však časovo náročné. Druhá možnosť, ktorú ponúkajú autori metódy, je založená na dvoch predpokladoch:

1. x-ová súradnica priesečníka kriviek R_M a R_{-M} je rovnaká ako x-ová súradnica priesečníka kriviek S_M a S_{-M}. Toto pravidlo zároveň vychádza z rovnice 4.1.

2. Krivky R_M a S_M sa pretínajú v bode, ktorý je určený vložením správy s dĺžkou rovnou polovici kapacity krycieho obrázka.

Na základe týchto dvoch predpokladov autori odvodili rovnicu pre výpočet dĺžky správy z počtu regulárnych a singulárnych skupín:

$$2(d_1 + d_0)x^2 + (d_0 - d_{-1} - d_1 - 3d_0)x + d_0 - d_0 = 0, \tag{4.2}$$

kde

$$\begin{aligned} d_0 &= R_M(p/2) - S_M(p/2), \\ d_1 &= R_M(1-p/2) - S_M(1-p/2), \\ d_{-0} &= R_{-M}(p/2) - S_{-M}(1-p/2), \\ d_{-1} &= R_{-M}(1-p/2) - S_{-M}(1-p/2). \end{aligned}$$

Dĺžka správy je potom vypočítaná ako

$$p = \frac{x}{x - \frac{1}{2}},$$

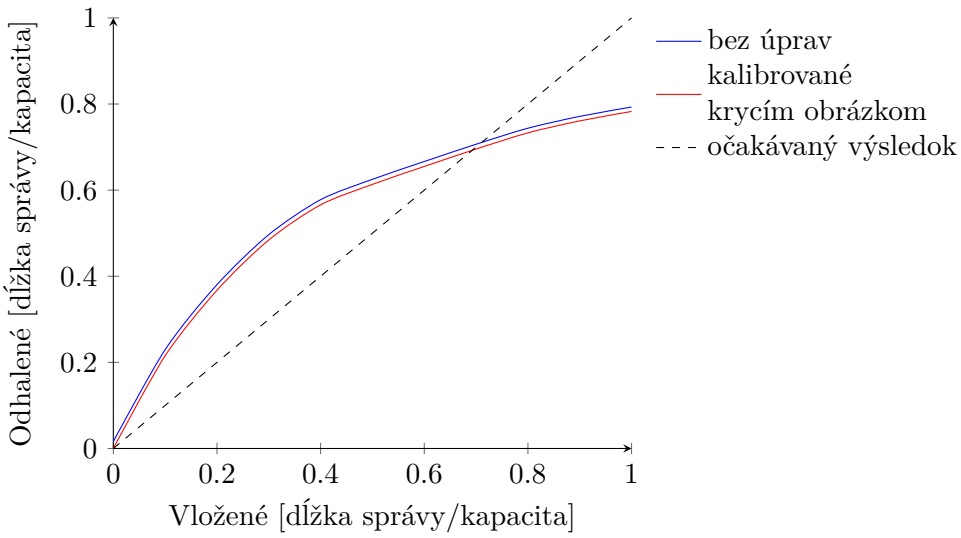
kde x predstavuje koreň rovnice 4.2, ktorého absolútna hodnota je nižšia.

Predpoklad, že hľadané krivky sú paraboly, však nemusí byť vždy správny. Zadaná kvadratická rovnica 4.2 nie je riešiteľná v obore reálnych čísel pre akýkoľvek stegoobrázok, keďže hodnota diskriminantu môže dosiahnuť záporné hodnoty. V takom prípade dôjde k aproximácii hľadaných kriviek ako priamok a hľadaným výsledkom je potom priemer x-ových súradníc priesečníkov priamok vyjadrujúcich počty regulárnych skupín a singulárnych skupín.

4.2.2 Experimentálne výsledky

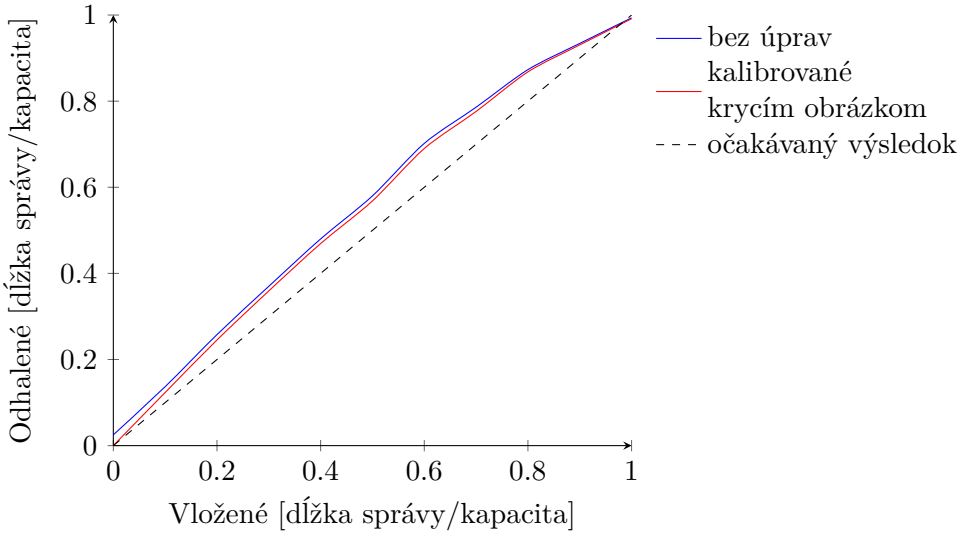
Testovanie stegoanalytickej metódy RS analýza prebiehalo s použitím dvoch sád obrázkov. Prvá sada bola tvorená farebnými fotografiami formátu PNG, vytvorenými pomocou mobilného telefónu LG Nexus 5X. Fotografie pôvodného formátu JPEG boli zmenšené a prevedené do formátu PNG. Veľkosť testovacej množiny bola 120 fotografií. Potom prebehlo ukrytie správy s dĺžkou 10-100% kapacity obrázka v 10% skokoch pomocou modifikovanej LSB metódy do každého obrázka. Stegoanalýzou pomocou RS analýzy bola odhadnutá dĺžka správy ukrytej v každom z farebných kanálov. Modifikovaná LSB metóda kóduje jeden bit informácie práve v jednom kanáli každého pixla, do ktorého má byť informácia ukrytá. Môžeme teda vyhlásiť, že kapacita tejto metódy vo farebných obrázkoch s tromi kanálmi je rovnaká ako kapacita jednokanálových sivotónových obrázkov. Ak chceme teda získať údaj hovoriaci o využití kapacity celého obrázka, je nutné sčítať výsledné odhadované dĺžky modrého a červeného kanála. Práve v nich sa totiž nachádzajú bity nesúce skrytú informáciu. Obrázok 4.6 zobrazuje pomer množstva odhalenej informácie a množstva informácie pôvodne vloženej do krycieho obrázka. Množstvo je vyjadrené ako pomer voči úplnej kapacite obrázka.

Druhou testovanou množinou boli fotografie pôvodného formátu JPEG, ktoré boli zmenšené, prevedené do odtieňov sivej a uložené vo formáte PNG. Veľkosť testovanej množiny bola 100 fotografií. Vzhľadom na fakt, že tieto fotografie obsahovali iba jeden kanál (intenzitu), na ukrytie informácie v krycom obrázku nebolo možné využiť modifikovanú LSB metódu, a teda ani náhodné vkladanie informácie. Použitou steganografickou metódou v tomto prípade bola teda sekvenčná metóda LSB 3.3. Vznikla tak možnosť zároveň otestovať aj schopnosti RS analýzy odhaľovať informáciu skrytú inou metódou. Podobne ako v prvom prípade boli postupne všetky obrázky naplnené informáciou s dĺžkou 10-100% kapacity obrázka v 10% skokoch. Potom boli všetky stegoobrázky analyzované RS analýzou, ktorá



Obr. 4.6: Odhadovaná veľkosť správy ukrytej modifikovanou metódou LSB pomocou RS analýzy.

určila množstvo skrytej správy tak v stegoobrázkoch, ako aj v krycích obrázkoch. Obrázok 4.7 ukazuje výsledky dosiahnuté RS analýzou tejto sady stegoobrázkov.



Obr. 4.7: Odhadovaná veľkosť správy ukrytej pomocou metódy LSB 3.3 v sivotónových obrázkoch.

Pre úplnosť je v tabuľke 4.1 zobrazená výkonnosť RS analýzy slepým prístupom voči modifikovanej LSB metóde. Ak vezmeme do úvahy fakt, že analýza nepozná parametre steganografickej metódy, nepozná ani jej kapacitu. Ak nepoznáme kapacitu stegoobrázka, je dobré uvažovať, že informácia môže byť uložená v celom obrázku. Dáta ukazujú, akú veľkú časť stegoobrázkov označila RS analýza ako tú, v ktorej sa nachádza tajná informácia. Zobrazujú teda pomer pixelov s tajnou správou voči všetkým pixelom obrázka, nie voči kapacite, ktorá vyplýva z použitej metódy.

obsah	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
odhad	0,07	0,12	0,16	0,19	0,20	0,22	0,23	0,24	0,25	0,26

Tabuľka 4.1: Odhadovaná dĺžka správy pri neznalosti použitej modifikovanej LSB metódy.

RS analýza nedosahuje dokonalé výsledky s ohľadom na odhadnutie dĺžky skrytej správy vo farebných stegoobrázkoch, ktoré boli pozmenené pomocou modifikovanej LSB metódy, a to najmä pri využití vyššej kapacity krycieho média. Podstatne lepšie výsledky dosahuje pri odhadovaní dĺžky správy zo stegoobrázkov vytvorených klasickou sekvenčnou metódou LSB. To je trochu prekvapivé, keďže samotní autori tejto metódy poznamenali, že výkon RS analýzy klesá so zvyšovaním sa výskytov kompaktných zhlukov ukrytej informácie [8], čo sekvenčná metóda LSB spĺňa – ukrýva informáciu od samého začiatku. Autori tvrdia, že RS analýza dosahuje lepšie výsledky v prípade, že skrytá informácia je rovnomerne rozprestretá v stegoobrázku. Toto tvrdenie nepodporuje zistenie z obrázka 4.6. Pri využití plnej kapacity obrázka sa skrýva informácia v celom modrom i červenom kanáli. Ak by sme predpokladali, že rozhodovanie medzi vložením informácie do jedného či druhého je aspoň trochu rovnomerné, čakali by sme rovnomerné rozloženie skrytej informácie – a teda podľa autorov najlepšie výsledky.

Tento predpoklad však nemusí byť pravdivý, keďže rozhodnutie o výbere kanála určeného na kódovanie je v réžii zeleného kanála. Súvislé plochy rovnakej farby tak môžu kódovať správu do rovnakého kanála a vytvárať tak zhluky skrytej informácie v oboch kanáloch. Táto situácia by podporovala záver autorov o nižšej výkonnosti RS analýzy pri odhaľovaní správ uložených v zhlukoch. Nezodpovedá však výsledkom, ktoré boli pozorované pri odhaľovaní sekvenčnej LSB steganografie.

Na druhej strane, RS analýza skvelo odhaľuje už malé množstvá skrytej informácie v stegoobrázkoch. Priemerná hodnota odhadovanej dĺžky správy v krycích obrázkoch je 0,0165 (čiže 1,65%) s najvyššou zaznamenanou hodnotou 0,04. Vzhľadom na fakt, že úlohou steganografie je utajiť samotnú prítomnosť akejkoľvek dodatočnej informácie, dá sa zhodnotiť, že aj keď RS analýza nemusí úplne presne odhadnúť dĺžku skrytej informácie, veľmi presne klasifikuje obrázky ako krycie alebo stegoobrázky.

Znalosť tejto odchýlky napomáha k spresneniu výsledku RS analýzy. Autori metódy použili dĺžku správy v krycom obrázku na kalibráciu výsledkov RS analýzy korešpondujúceho stegoobrázku. Skutočnú dĺžku správy l potom predstavuje

$$l = \frac{l_{det} - l_{init}}{1 - l_{init}},$$

kde l_{det} je detegovaná dĺžka skrytej správy RS analýzou v stegoobrázku a l_{init} predstavuje dĺžku správy v krycom obrázku. Na obrázkoch 4.6 a 4.7 sa nachádzajú oba výsledky – detegovaná dĺžka správy v stegoobrázku i upravená dĺžka. Tá bola určená s ohľadom na množstvo chybne identifikovaného množstva skrytej informácie v korešpondujúcom krycom obrázku.

4.3 Hmotný bod charakteristickej funkcie histogramu

Stegoanalytické metódy zaoberajúce sa odhaľovaním metód nahradzujúcich LSB (3.3, 3.4) sú pomerne známe a dosahujú veľmi dobré výsledky. Podstatne menej detektorov však bolo predstavených pre metódy ±1 vkladania. Na prvý pohľad sa môže zdať, že predstavené

metódy pre LSB by mohli dosahovať podobné výsledky aj pre odhaľovanie ±1 vkladania, keďže to vnáša do krycieho obrázka steganografický šum podobne ako iné LSB metódy. Tabuľka 4.2 však ukazuje pravý opak. Dôvodom je, že spomenuté metódy využívajú na odhalenie steganografie symetriu susedných hodnôt, ktorú táto steganografia zanáša do histogramu krycieho obrázka. Metóda ±1 vkladania však takúto symetriu neprináša, keďže povoľuje pri nezhode najnižších bitov hodnotu pixelu znížiť i zvýšiť o 1. V histograme sa tak nevytvárajú vedľa seba dvojice početnosti hodnôt pixelov, ktoré sa k sebe badateľne približujú hodnotou.

stegoanalytická metóda	TPR	FPR
χ^2 test	0,7%	3,1%
RS analýza	4,3%	5,2%

Tabuľka 4.2: Úspešnosť LSB stegoanalytických metód pri odhaľovaní ±1 vkladania.

Na odhalenie ±1 vkladania je tak potrebný iný prístup než skúmanie pomerov hodnôt histogramu. Jednou z možností je analýza charakteristickej funkcie histogramu a jej hmotného bodu (ďalej ako COM z angl. centre of mass). Autor tejto metódy [11] využil transformáciu histogramu a histogramu susedstva pixelov na odhalenie prítomnosti steganografických metód LSB vrátane ±1 vkladania.

4.3.1 Popis metódy

Krycí obrázok pozostáva z pixelov s intenzitou $0, \ldots, N-1$, kde N predstavuje najvyššiu hodnotu intenzity pixelu (pre potreby tejto metódy budeme predpokladať čiernobiele obrázky). Hodnotu pixelu krycieho obrázku môžeme vyjadriť ako $p_c(i,j)$, kde (i,j) predstavuje pozíciu pixelu v obrázku. Pridaním dodatočnej informácie do tohto pixelu následne získavame stegopixel, ktorého hodnotu predstavuje $p_s(i,j)$. Histogram obrázka pomocou hodnoty pixelov môžeme vyjadriť ako

$$h(n) = |\{(i,j)|p(i,j) = n\}|.$$

Histogram krycieho obrázka predstavuje $h_c(n)$ a histogram stegoobrázka podobne $h_s(n)$. Položme teda $H[k]$ ako diskrétnu Fourierovu transformáciu (ďalej ako DFT) signálu $h(n)$. Získame tak frekvenčnú charakteristiku histogramu, $H_c[k]$ pre krycí obrázok a $H_s[k]$ pre stegoobrázok. Táto charakteristika je nazývaná charakteristickou funkciou histogramu (ďalej uvádzané ako HCF z angl. histogram characteristic function).

Steganografia vnáša do krycieho obrázka určitý šum. Za pomoci histogramu môžeme vyjadriť histogram stegoobrázka nasledujúcou konvolúciou pravdepodobnostných funkcií

$$h_s = h_c * f,$$

kde f predstavuje pravdepodobnostnú funkciu vkladaného šumu. Pre HCF potom platí

$$H_s[k] = H_c[k]F[k]. \tag{4.3}$$

Rozloženie šumu v prípade metódy ±1 vkladania predstavuje $f(0) = 0,5, f(\pm 1) = 0,25$, z čoho vyplýva, že

$$F[k] = cos^2(\pi k/N). \tag{4.4}$$

Je to spôsobené faktom, že štatisticky sa v polovici prípadov bit zmeniť nemusí – vkladaný bit odpovedá bitu krycieho obrázka. V druhej polovici vzniká nutnosť bit zmeniť. Metóda

± 1 vkladania pri zmene bitu hodnotu pixelu zvýši alebo zníži o 1. Rozhodnutie o znížení alebo zvýšení hodnoty pixelu je náhodné, no má uniformné rozloženie, preto hodnoty $+1$ aj -1 majú hodnotu 0,25. Hodnota tejto funkcie nie je nikdy väčšia ako 1 a $H_s[k]$ bude teda nanajvýš rovné $H_c[k]$. Hodnota funkcie sa takisto blíži 0 pre k blížiace sa $N/2$. Môžeme teda prehlásiť, že pre vysoké k bude $H_s[k]$ významne nižšie ako $H_c[k]$. Tento fakt sa dá použiť na odhalenie steganografického šumu v stegoobrázku [9]. Jeho prítomnosť sa dá detegovať pomocou hmotného bodu definovaného ako

$$C(H[k]) = \frac{\sum_{i=0}^{n} i|H[i]|}{\sum_{i=0}^{n} |H[i]|},$$

kde $n = N/2$, vzhľadom na symetriu DFT reálnych signálov. Keďže vieme, že pre každé k platí $H_s[k] < H_c[k]$, musí potom platiť aj

$$C(H_s[k]) < C(H_c[k]).$$

Tento vzťah je základom detektorov odhaľujúcich steganografický šum zanesený do obrázka pomocou ± 1 vkladania. Hlavnou nevýhodou odhaľovania steganografie iba pomocou HCF COM je fakt, že vo veľmi veľkej väčšine prípadov má analytický nástroj k dispozícii iba potenciálny stegoobrázok. Keďže nedisponuje krycím obrázkom, nedokáže určiť hodnotu $C(H_c[k])$. Zo samotnej hodnoty $C(H_s[k])$ nie je možné vydedukovať, či je obrázok ovplyvnený steganografiou alebo nie. Sivotónové obrázky nemajú dostatočnú variabilitu, akou disponujú obrázky farebné. Histogramy farebných obrázkov sú často riedke a vyznačujú sa zhlukmi farieb, na rozdiel od nich histogramy obrázkov v odtieňoch sivej často pripomínajú šum, a tak rozdiely medzi $C(H_c[k])$ a $C(H_s[k])$ nemusia byť dostatočne veľké na to, aby mohli byť klasifikované bez vzájomného porovnania. Taktiež sa hodnoty $C(H_c[k])$ medzi rôznymi krycími obrázkami líšia natoľko, že hodnoty korešpondujúcich $C(H_s[k])$ nie sú žiadnym dostatočne presným spôsobom klasifikovateľné.

Vysoká variabilita COM a absencia krycieho obrázka

Problém vysokej variability hodnôt $C(H_c[k])$ i absencie obrázka, do ktorého bola vložená steganografická informácia, je možné odstrániť. Využijeme na to zmenšený obrázok, ktorý získame z pôvodného obrázka nasledujúcim spôsobom:

$$p'(i,j) = \left\lfloor \sum_{u=0}^{1} \sum_{v=0}^{1} \frac{p_c(2i+u, 2j+v)}{4} \right\rfloor,$$

kde $p'(i,j)$ predstavuje pixel zmenšeného obrázka. Následne vyrátame HCF a COM zmenšeného obrázka a získame teda $H_c^{'}[k]$ a $C(H_c^{'}[k])$. Podľa [11] sa COM zmenšeného obrázka od COM obrázka pôvodného nelíši významným spôsobom za predpokladu, že je tento obrázok krycí a teda neovplyvnený steganografickým šumom:

$$C(H_c^{'}[k]) \approx C(H_c[k]).$$

Zmenšením stegoobrázka nedôjde k úplnej eliminácii steganografického šumu. Zachovanie aspoň určitého množstva šumu prispieva k modifikácii HCF a následne k zníženiu COM v zmenšenom stegoobrázku, no v podstatne nižšej miere než v pôvodnom stegoobrázku. Dá sa teda poznamenať, že platí:

$$C(H_c^{'}[k]) - C(H_s^{'}[k]) < C(H_c[k]) - C(H_s[k]).$$

Z týchto rovníc teda vyplýva, že ak bol obrázok ovplyvnený steganografiou (bol do neho zanesený steganografický šum), tak pre neho a jeho zmenšenú verziu platí vzťah:

$$C(H_s^{'}[k]) > C(H_s[k]).$$

Výslednú hodnotu určujúcu, či obrázok je alebo nie je stegoobrázkom, predstavuje bezrozmerný diskriminátor $C(H_s[k])/C(H_s^{'}[k])$. Zmenšený obrázok tak kalibruje COM pôvodného obrázka. Táto kalibrácia umožňuje vzájomné porovnanie aj takých obrázkov, ktorých hodnoty COM sa veľmi líšia.

Hustota a kompaktnosť histogramu

Histogram čiernobieleho obrázka nevykazuje vlastnosti histogramov farebných obrázkov. Často býva kompaktný, na rozdiel od histogramov farebných obrázkov, ktoré bývajú riedke. Túto vlastnosť však vieme umelo vytvoriť aj v histograme čiernobieleho obrázka. Využijeme na to dvojrozmerný histogram susedných hodnôt pixelov:

$$h^2(m,n) = |\{(i,j)|p(i,j) = m, p(i,j+1) = n\}|.$$

Vzhľadom na fakt, že susedné pixely majú často podobné hodnoty, vytvára sa na diagonále histogramu zhluk hodnôt a mimo diagonály je histogram riedky.

Steganografický šum tento histogram ovplyvňuje podobným spôsobom ako je ovplyvnený obyčajný histogram. Môžeme teda použiť metódu HCF COM, avšak s využitím dvojrozmernej DFT. S jej využitím dostaneme HCF $H^2[k,l]$, z ktorej by sme mohli získať COM, v tomto prípade by však bol dvojrozmerný. Na kalibráciu pomocou zmenšeného obrázka a výpočet bezrozmerného diskriminátora je však nutné určitým spôsobom pretransformovať dvojrozmerný COM. S pomocou jediného kvadrantu dvojrozmernej HCF získavame vzťah [11]:

$$C^2(H^2[k,l]) = \frac{\sum_{i,j=0}^{n}(i+j)|H^2[i,j]|}{\sum_{i,j=0}^{n}|H^2[i,j]|}.$$

Tento spôsob výpočtu COM nahrádza pôvodný výpočet v metóde zmenšovania obrázka a podľa [11] platia všetky spomenuté vzťahy pre COM zmenšeného a pôvodného obrázka rovnako.

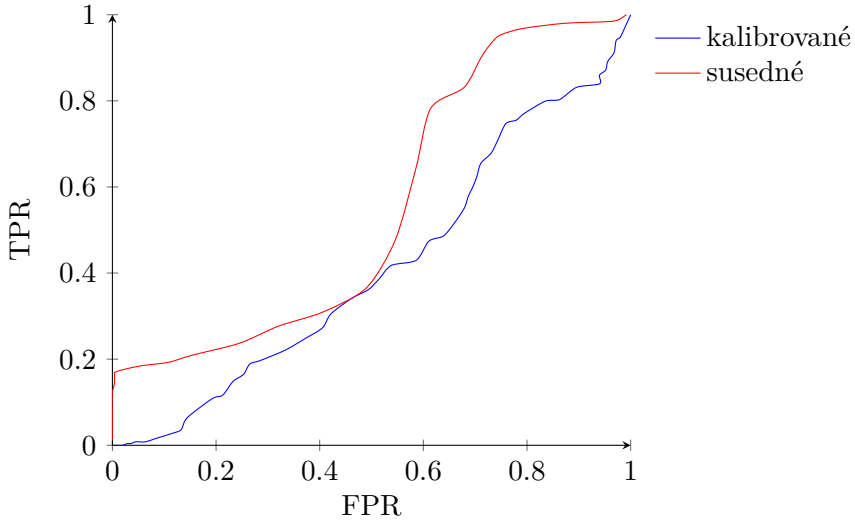
4.3.2 Experimentálne výsledky

Obe metódy (kalibrácia HCF COM i kalibrácia HCF COM pomocou histogramu susedných pixelov) boli testované na dvoch sadách obrázkov formátu PNG. Obe sady boli vytvorené zmenšením fotografií formátu JPEG a ich prevodom do odtieňov sivej. Rozdielom okrem početnosti v týchto sadách bol zdroj – obe boli vyfotografované iným prístrojom. Menšia sada bola zachytená pomocou fotoaparátu mobilného telefónu LG Nexus 5X a obsahovala približne 230 fotografií (ďalej ako sada L). Väčšia sada bola vyfotografovaná pomocou mobilného telefónu Samsung Galaxy S5 mini a obsahovala približne 830 fotografií (ďalej ako sada S).

Experiment pozostával z klasifikovania obrázkov pomocou výsledného diskriminantu. Vykonaný bol pre každú sadu obrázkov dvakrát. Najprv prebiehala analýza obrázkov, do ktorých bola vložená informácia s maximálnou dĺžkou a teda bola naplnená kapacita krycieho obrázka. V druhom prípade bola kapacita krycieho obrázka využitá na 50%.

Výsledky kompletnej sady L s využitím plnej kapacity krycích obrázkov sú s ohľadom na výsledky prezentované v [11] nedostatočné. Na obrázku 4.8 je viditeľné, že krivky oboch

metód sa nachádzajú pod funkciou $y = x$. Analýzou diskriminantov a hlavne COM jednotlivých obrázkov je viditeľné, že steganografický proces má zanedbateľný vplyv na stegoobrázky, ktoré boli vytvorené z krycích obrázkov s nízkym COM. Vysvetlenie je možné hľadať v rovnici popisujúcej HCF stegoobrázka 4.3 a rovnici popisujúcej charakteristiku šumu 4.4. Steganografický proces má výrazný vplyv na nízke frekvencie. Práve posilnenie nízkych frekvencií znižuje COM HCF. Ak však HCF samotného krycieho obrázka obsahuje dominantné nízke frekvencie, nie je čo posilňovať, resp. posilnenie takýchto dominantných frekvencií už nemá za následok dramatickú zmenu COM, ktorú by bolo možné detegovať.



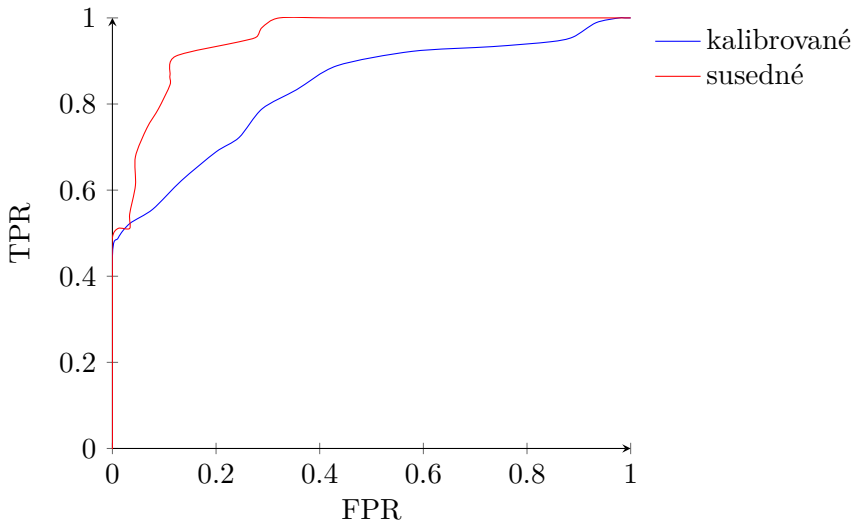
Obr. 4.8: ROC krivky HCF COM detektora pre sadu L.

Na obrázku 4.9 je ROC krivka upravenej sady L. Z tejto sady boli vylúčené také krycie obrázky, ktorých COM je menší ako 12. O týchto obrázkoch môžeme prehlásiť, že v ich HCF dominujú nízke frekvencie. Tvar ROC kriviek napovedá, že predpoklad o nutnosti relatívne vysokej hodnoty COM na odhalenie manipulácie obrázka pomocou steganografických metód je správny. Na základe dvojice hodnôt COM a diskriminantu je potom možné určiť, či obrázok obsahuje skrytú informáciu alebo nie. Ak je však hodnota diskriminantu blízka 1 a hodnota COM je nízka, nevieme s istotou o obrázku prehlásiť nič. V prípade, že je hodnota diskriminantu aj COM nízka, môžeme povedať, že je obrázok stegoobrázkom.

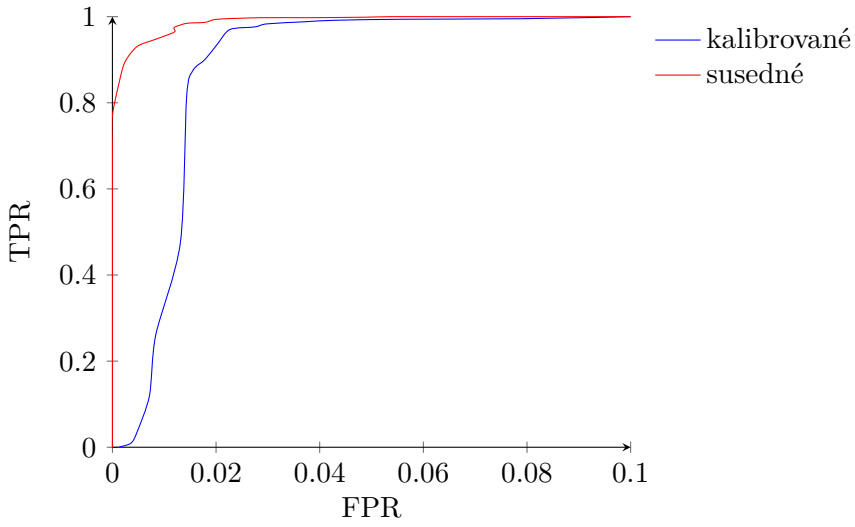
Na obrázku 4.10 sú výsledky získané z obrázkov zo sady S s využitím plnej kapacity. Takmer všetky obrázky tejto sady mali vysokú hodnotu COM a detektor potvrdil predpoklad položený pri predchádzajúcom experimente. Hodnoty ROC kriviek naznačujú minimálne počty false positives pri zachovaní veľmi vysokej schopnosti detektora odhaliť stegoobrázky. Mierka grafu zobrazuje iba relevantnú časť celého grafu.

Na obrázkoch 4.11 a 4.12 je zobrazaná úspešnosť detektorov pri detegovaní steganografie s využitím približne polovičnej kapacity krycieho obrázka. Z ROC kriviek v obidvoch grafoch je znateľné, že využívanie kapacity krycieho obrázka má výrazný vplyv na odhalenie steganografických modifikácií, ktoré naň boli aplikované. Čím rozsiahlejšia informácia sa v stegoobrázku skrýva, tým ľahšie ju HCF COM detektor odhalí. Tento efekt je viditeľnejší práve na sade S, pri ktorej s využitím plnej kapacity dosahoval detektor skvelé výsledky, no pri skrátení skrytej informácie na polovicu sa výsledky zhoršili.

Pre sadu L platí, že výsledky ostali viacmenej nezmenené, no táto sada (hlavne podmnožina spĺňajúca podmienku $COM > 12$) je podstatne menšia, a teda štatisticky menej



Obr. 4.9: ROC krivky HCF COM detektora pre upravenú sadu L.

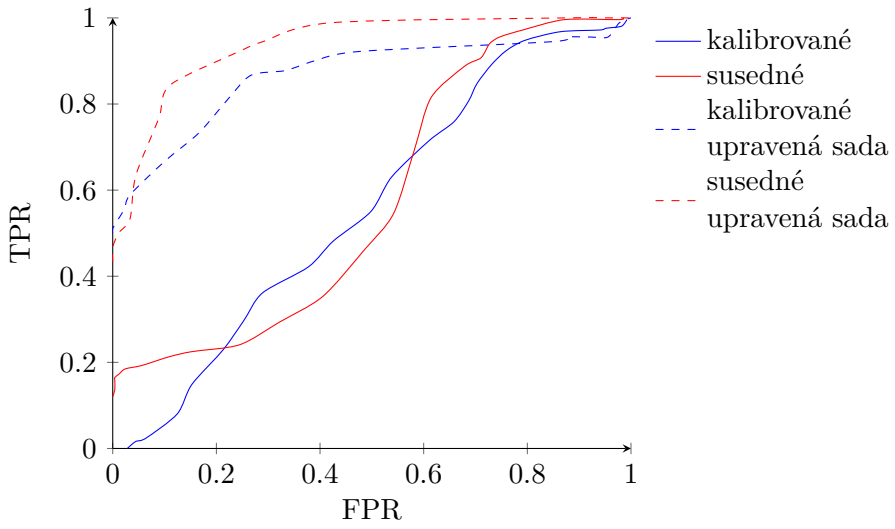


Obr. 4.10: ROC krivky HCF COM detektora pre sadu S.

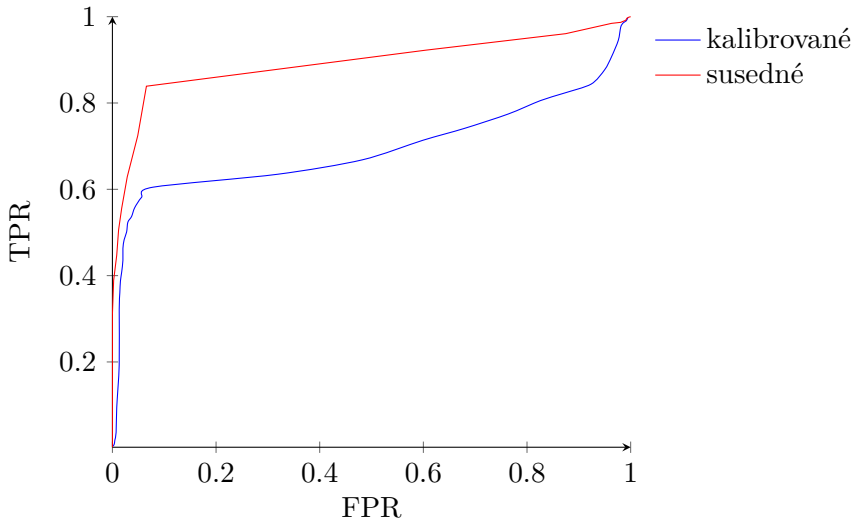
presná. Takisto môže byť dôvodom dobrej výkonnosti aj samotná vybraná podmnožina obrázkov, ktorá spĺňa kritériá pre ľahké odhalenie. Keďže ani mohutnosť tejto množiny nie je vysoká, výsledky získané pomocou sady S, ktorá obsahuje asi dvanásťnásobok počtu obrázkov upravenej sady L, môžu byť považované za relevantný ukazovateľ toho, že kratšia skrytá informácia vedie k zníženej pravdepodobnosti odhalenia steganografickej metódy aplikovanej na krycí obrázok.

4.4 Porovnanie stegoanalytických metód

V podkapitole 3.6 je opísaná metóda susedov, ktorá nie je typickým predstaviteľom LSB steganografie. Výber tejto metódy a jej implementácia mali za úlohu ukázať nedostatky



Obr. 4.11: ROC krivky HCF COM detektora pre sadu L s využitím polovičnej kapacity.



Obr. 4.12: ROC krivky HCF COM detektora pre sadu S s využitím polovičnej kapacity.

LSB stegoanalytických štatistických metód. Na nasledujúcich riadkoch sa nachádza krátky popis výsledkov dosiahnutých pomocou metód popísaných v kapitole 4.

χ^2 test

Metóda χ^2 test pri odhaľovaní steganografie zavedenej pomocou metódy susedov zlyháva vo všetkých prípadoch. Hlavným dôvodom je ten, že metóda susedov nevyberá pixely, do ktorých je uložená tajná správa sekvenčne – zmenený je iba každý druhý pixel v riadkoch i stĺpcoch. Druhým dôvodom je, že hodnoty zmenených pixelov sa nemenia v pároch, ktoré by vytvárali symetriu susedných hodnôt histogramu. Táto situácia môže nastať v najhoršom prípade, keď je do každého vybraného pixla vložený práve jeden bit (keď je obrázok zložený z intenzít s veľmi malou odchýlkou). Ani vtedy však χ^2 test manipuláciu s obrázkom

neodhalí, kvôli prvému dôvodu. Experimentálny dôkaz je podaný v podkapitole 4.1, kde sa nachádzajú výsledky testovania obrázka s nesekvenčným vkladaním informácie.

RS analýza
RS analýza ponúka najlepšie výsledky s ohľadom na detekciu prítomnosti akejkoľvek informácie v bežnom krycom obrázku. Táto metóda totiž odstraňuje najväčšiu slabinu χ^2 testu – neschopnosť odhaliť nesekvenčné vkladanie skrývanej informácie. Za predpokladu, že obrázok nie je členitý (nachádzajú sa v ňom súvislé plochy, ktoré majú rovnakú alebo veľmi podobnú intenzitu), metóda susedov vo veľkej väčšine pixelov môže vložiť iba jeden bit informácie. Práve tieto pixely potom RS analýza odhalí. Nedokáže však spoľahlivo určiť dĺžku ukrytej správy a pri použití zašumeného krycieho obrázka nedokáže odhaliť ani samotnú prítomnosť vloženej správy, keďže tá sa často nachádza vo viacerých bitoch vybraných pixelov.

HCF COM detektor
Táto metóda sa zameriava na odhaľovanie šumu, ktorý je zanesený do krycieho obrázka pomocou ± 1 metódy. Tento steganografický šum má špecifickú pravdepodobnostnú funkciu, o ktorú sa opierajú základné predpoklady HCF COM detektora. Metóda susedov však do obrázka zanáša šum s inou pravdepodobnostnou funkciou – zmeny pixelov sa pohybujú vo väčšom rozsahu ako $\langle -1, 1 \rangle$. Frekvenčná charakteristika obrázka sa nemení spôsobom, na ktorý sa zameriava HCF COM detektor. Výsledky analýzy pomocou HCF COM detektora sú teda veľmi závislé na členitosti krycieho obrázka – čím je obrázok členitejší, tým menej pixelov je zmenených spôsobom podobným ± 1 vkladaniu a tým nižšia je šanca, že bude odhalená manipulácia s krycím obrázkom.

Vo všeobecnosti sa však dá povedať, že metódy RS analýzy a HCF COM dosahujú pre bežné krycie obrázky ovplyvnené metódou susedov prijateľné výsledky v odhalení prítomnosti správy. Takéto obrázky totiž obsahujú vysoké množstvo pixelov, do ktorých je možné vložiť iba jeden bit informácie. Malou modifikáciou metódy susedov však vieme eliminovať schopnosť detegovať ukrytú správu. Jednou možnosťou je zvýšiť minimálny počet vkladaných bitov na dva, druhou je využívať druhý najmenej významný bit. Oba prístupy znižujú vizuálnu kvalitu obrázka, no znižujú úspešnosť RS analýzy i HCF COM detektora. Výsledky získané pomocou stegoanalytických metód pri odhaľovaní metódy susedov sa nachádzajú v tabuľke 4.3.

	bez zmeny	2 bity	predposledný bit
χ^2 test	0	0	0
RS analýza	0,22	0,13	0
HCF COM	0,90	0,98	1,02

Tabuľka 4.3: Výsledky stegoanalytických metód pri odhaľovaní metódy susedov a jej modifikácií.[3]

[3] RS analýza, χ^2 test – čím vyššie, tým lepšie; HCF COM – čím nižšie, tým lepšie.

Kapitola 5

Implementácia steganografických a stegoanalytických metód

Pre potreby implementácie steganografických a stegoanalytických metód bol vybraný programovací jazyk Python vo verzii 3.6. Na otváranie obrázkov, ich spracovanie a ukladanie bola využitá knižnica PIL vo verzii 1.1.7. Všetky obrázky použité na testovanie dosahovali maximálne rozlíšenie 914 pixelov na šírku a 514 pixelov na výšku.

Výber steganografických metód určených na implementáciu bol vykonaný s ohľadom na zvyšujúcu sa teoretickú náročnosť ich odhalenia. Všetky vybrané metódy operujú v priestorovej doméne digitálnych obrázkov. Vybranými metódami boli:

- LSB,
- modifikovaná metóda LSB,
- ± 1 vkladanie,
- metóda susedov.

Výber bol podnietený faktom, že každá metóda odstraňuje určitú štatistickú vlastnosť predchádzajúcej metódy, ktorá umožňuje jej odhalenie pomocou špecifickej stegoanalytickej funkcie. Zámerom bolo poukázať na nutnosť vývoja stegoanalytických funkcií v náväznosti na posun v oblasti steganografie. V podkapitolách nazvaných *Experimentálne výsledky* sú výsledky odhaľovania steganografických metód pomocou jednotlivých stegoanalytických metód. V podkapitole 4.4 je následne uvedené porovnanie úspešnosti v odhaľovaní adaptívnej steganografickej metódy.

Pre každú steganografickú metódu bol vytvorený samostatný modul. V prípade metód zaoberajúcich sa LSB steganografiou (metódy LSB, modifikovaná LSB a ± 1 vkladanie) obsahuje každý modul definíciu jednej triedy a troch funkcií. Trieda je zodpovedná za kódovanie jednotky skrývanej informácie (jedného bitu) na správnu pozíciu, čítanie zakódovanej správy a určenie kapacity krycieho obrázka. Funkcie v moduloch LSB steganografie majú za úlohu zakódovať celú správu, prečítať správu zo zadaného obrázka a zistiť kapacitu daného obrázka. Kapacita je udaná ako počet znakov najdlhšej správy, ktorá sa do obrázka zmestí bez jej skrátenia. Tieto funkcie zaobaľujú vytvorenie inštancie triedy a volania jej metód. Modul metódy susedov obsahuje podobne tri funkcie s rovnakou funkcionalitou – zakódovanie a prečítanie správy a určenie kapacity obrázka.

Všeobecný postup funkcie zakódovania je vytvorenie zoznamu bitov, z ktorých sa skladá tajná správa. Obsah správy je definovaný buď parametrom programu alebo sa číta zo štan-

dardného vstupu. Potom sa určí dĺžka tajnej správy a uloží sa do prvých 32 bitov určených pre uloženie informácie do stegoobrázka. Následne sa uloží celá správa bit po bite, až do vyčerpania kapacity obrázka, alebo zoznamu bitov. Uložená dĺžka neskrátenej správy pri dekódovaní napovie adresátovi, či správa bola alebo nebola skrátená. V prípade, že dĺžka správy prekročila kapacitu obrázka, program túto skutočnosť oznámi na štandardný chybový výstup. Pri dekódovaní je obsah ukrytej správy vypísaný na štandardný výstup.

V prípade modifikovanej metódy LSB je pridaná možnosť ukladať správu s pomocou kľúča. Ak sa táto možnosť využije, nerozhoduje sa o výbere kanála len pomocou bitu zo zeleného kanála, ale aj pomocou bitu kľúča. Použitie tajného zdieľaného kľúča pridáva kryptografický rozmer a zvyšuje dôvernosť, no nemá žiadny pozorovaný vplyv na neodhaliteľnosť správy v bežných obrázkoch. Ak by LSB zeleného kanála boli bity rovnakej hodnoty (bežné obrázky to nespĺňajú), viedlo by to k odhaleniu správy pomocou χ^2 testu. Potom tajný kľúč vytvorí pseudonáhodnú postupnosť, podľa ktorej sa bude voliť kanál pre uloženie bitov správy.

Všetky steganografické metódy využívajúce LSB princíp majú časovú zložitosť v triede $O(n)$ a zložitosť závisí na dĺžke správy. Metóda susedov má polynomiálnu časovú zložitosť, pretože pri skúmaní okolia jednotlivých pixelov musí pracovať s preskúmanými pixelmi viacnásobne (dva- až štyrikrát).

Výber implementovaných stegoanalytických metód korešpondoval s výberom steganografických metód. S výnimkou metódy susedov bola pre každú steganografickú metódu implementovaná taká stegoanalytická metóda, ktorá ju dokáže odhaliť. Implementované boli všetky metódy z kapitoly 4:

- χ^2 test na odhalenie LSB,
- RS analýza na odhalenie modifikovanej LSB metódy,
- HCF COM detektor na odhalenie ± 1 vkladania.

Každá stegoanalytická metóda sa nachádza vo vlastnom module. Výstupom metód χ^2 testu a RS analýzy je pomer odhadovanej dĺžky správy ukrytej v obrázku v porovnaní s kapacitou obrázka, ktorý bol modifikovaný sekvenčnou LSB metódou. Výstupom HCF COM detektoru je dvojica diskriminantov získaných zo zmenšeného obrázka a histogramu susedov zmenšeného obrázka. Čím vyššia hodnota tohto diskriminantov, tým nižšia pravdepodobnosť, že obrázok je stegoobrázkom. V prípade farebného obrázka vracia RS analýza a HCF COM detektor trojicu výsledkov – pre každý kanál jeden.

Popis obsluhy a spustenia implementovaných programov sa nachádza v prílohe A.

Kapitola 6

Záver

V tejto práci boli priblížené pojmy steganografie a stegoanalýzy. Prínos steganografie k utajovaniu informácií je nazanedbateľný. Aj keď sa môže zdať, že najväčší rozkvet má toto odvetvie za sebou, ani v dnešnej dobe jej význam neklesá. Dôkazom nech je pokrok a výskum v oblasti sieťovej steganografie.

Tak ako postupuje vývoj steganografie, nesmie sa zastaviť ani pokrok v oblasti stegoanalýzy. Ilegálne aktivity využívajú všetky poskytnuté nástroje a s príchodom sofistikovanejších metód je nutné držať krok v ich odhaľovaní. Stegoanalýza je tak veda, ktorej je dnes venovaná ešte väčšia pozornosť ako kedykoľvek predtým. Masové využitie sieťovej steganografie bude vyžadovať veľké úsilie na úspešné odhalenie a obranu voči útokom vykonaným s jej pomocou.

Práca zahŕňa prehľad steganografických metód, jednotlivých oblastí steganografie, priblíženie princípov stegoanalýzy a klasifikáciu stegoanalytických metód. Ďalej sa v práci nachádza skupina steganografických a stegoanalytických metód s popisom ich princípov a vlastností z oblasti obrazovej steganografie. Týmito metódami sú LSB a jej modifikácia, ± 1 vkladanie (známe tiež ako LSB matching) a metóda susedov ako zástupcovia steganografie a metóda RS, analýza HCF COM a χ^2 test, ktoré reprezentujú stegoanalytické metódy využívané na odhaľovanie spomenutých steganografických metód.

Jedným z cieľov práce bolo poukázanie na nutnosť pokroku v oblasti stegoanalýzy. Výsledky práce zahŕňajú overenie teoretických vlastností steganografických metód a ich odolnosti voči stegoanalytickým metódam určeným na odhaľovanie menej sofistikovaných postupov. Vzhľadom na fakt, že stegoanalytické metódy implementované v práci zlyhávajú pri odhaľovaní steganografie na vyššej úrovni, môžeme konštatovať, že tento cieľ bol naplnený. Bez pokroku v oblasti stegoanalýzy, či už slepej alebo cielenej, sa nové steganografické metódy nebudú dať odhaliť a boj proti nim bude neefektívny.

Literatúra

[1] Anckaert, B.; Sutter, B. D.; Bosschere, K. D.: *Steganography for Executables*. Január 2005, [Online; navštívené 3.1.2018].
URL https://www.researchgate.net/publication/242404201_Steganography_for_Executables

[2] Boutel, T.: *PNG (Portable Network Graphics) Specification Version 1.0*. Internet Requests for Comments, Marec 2007, [Online; navštívené 3.1.2018].
URL https://tools.ietf.org/html/rfc2083

[3] Cancelli, G.: *New techniques for steganography and steganalysis in the pixel domain*. Dizertačná práca, Universita degli Studi di Siena, Dipartimento di Ingegneria dell'Informazione, Máj 2009.

[4] Chang, C.-C.; Chen, T.-S.; Chung, L.-Z.: A steganographic method based upon JPEG and quantization table modification. *Information Sciences*, ročník 141, č. 1-2, Marec 2002.

[5] Cheddad, A.; Condell, J.; Curran, K.; aj.: Digital image steganography: Survey and analysis of current methods. *Signal Processing*, ročník 90, 2010.

[6] Chiew, K. L.: *Steganalysis of binary images*. Dizertačná práca, Macquire University, Faculty of Science, Jún 2011.

[7] Das, S.; Johri, P.; Kumar, A.; aj.: Survey on Steganography Methods (Text, Image, Audio, Video, Protocol and Network Steganography). In *International Confrerence on Computing for Sustainable Global Development (INDIACom)*, 2016, ISBN 978-9-3805-4421-2.

[8] Fridrich, J.; Goljan, M.; Du, R.: Detecting LSB steganography in color, and gray-scale images. *IEEE MultiMedia*, ročník 8, č. 4, December 2001.

[9] Harmsen, J.; Pearlman, W.: Hihger-order statistical steganalysis of palette images. *Proc. SPIE Security Watermarking Multimedia Contents*, ročník 5020, 2003.

[10] Jayaram, P.; Ranganatha, H. R.; Anupama, H. S.: Information hiding using audio steganography – a survey. *The International Journal of Multimedia and Its Applications*, ročník 3, č. 3, August 2011.

[11] Ker, A. D.: Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, ročník 12, č. 6, Jún 2005.

[12] Krishan, R. B.; Thandra, P. K.; Baba, M. S.: An overview of text steganography. In *Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, 2017, ISBN 978-1-5090-4740-6.

[13] Kumar, M.: *Steganography and steganalysis of joint picture expert group (JPEG) images*. Dizertačná práca, University of Florida, 2011.

[14] Mazurczyk, W.; Szczypiorski, K.; Zielińska, E.: Trends in Steganography. *Communications of the ACM*, ročník 57, č. 3, Marec 2014.

[15] Poremba, T.: *Digitální steganografie a stegoanalýza*. Semestrálny projekt, Vysoké učení technické v Brně, Fakulta informačních technologií, 2018.

[16] Swain, G.: Steganography in Digital Images Using Maximum Difference of Neighboring Pixel Values. *International Journal of Security and its Applications*, November 2013.

[17] Westfeld, A.; Pfitzmann, A.: Attacks on Steganographic Systems. In *International Workshop on Information Hiding*, ročník 1768, Springer, Berlin, Heidelberg, Marec 2000.

[18] Zhou, X.; Gong, W.; Fu, W.; aj.: An improved method for LSB based color image steganography combined with cryptography. *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, Jun 2016.

Príloha A

Spustenie a obsluha implementovaných programov

Všetky vytvorené programy sú implementované v jazyku Python vo verzii 3.6. Nutnou podmienkou pracovania s vytvorenými programami je prítomnosť knižnice PIL vo verzii 1.1.7. Program pracuje s obrázkami formátu PNG. Modifikovaná metóda LSB vyžaduje farebné PNG obrázky. Metóda susedov bola testovaná pre sivotónové PNG obrázky.

A.1 steganography.py

Príklad spustenia:
`python steganography.py -e -M lsb -m message -i fileIn.png -o fileOut.png`

Popis prepínačov:

- `-h, --help` vytlačí nápovedu,
- `-e, --encode` zvolí vkladanie skrývanej informácie,
- `-d, --decode` zvolí extrakciu skrytej informácie,
- `-c, --capacity` zvolí výpočet kapacity obrázka,
- `-i INPUT, --input` názov vstupného súboru, povinné,
- `-o OUTPUT, --output` názov výstupného súboru, len pre vkladanie,
- `-m MESSAGE, --message` obsah skrývanej správy,
- `-M METHOD, --method` metóda skrývania,
- `-k KEY, --key` kľúč, relevantné len pre metódu `lsb2`,
- `-t TYPE, --type` podtyp metódy susedov.

Pre metódu skrývania sú možné hodnoty `lsb`, `lsb2`, `matching` alebo `neighbours`. Pre podtyp metódy susedov sú možné hodnoty 5, 6, 7 alebo 8. Východzia hodnota je 5. Pri absencii prepínača `-m` sa obsah skrývanej správy číta zo štandardného vstupu. Prepínače `-e`, `-d` a `-c` sa vzájomne vylučujú. Pri zvolení prepínača `-d` alebo `-c` sa výsledok vytlačí na štandardný výstup.

A.2 steganalysis.py

Príklad spustenia:
`python steganalysis.py -M chi2 -i fileIn.png`

Popis prepínačov:

- `-h, --help` vytlačí nápovedu,
- `-i INPUT, --input` názov vstupného súboru,
- `-M METHOD, --method` metóda odhaľovania.

Pre metódu odhaľovania sú možné hodnoty `chi2`, `rs` alebo `hcf`. Výsledok sa tlačí na štandardný výstup. V prípade metódy `chi2` je vypísaná odhadovaná dĺžka správy vzhľadom na kapacitu obrázka. V prípade metódy `rs` je vypísaná odhadovaná dĺžka správy po jednotlivých kanáloch obrázka vzhľadom na kapacitu kanála. V prípade metódy `hcf` je vypísaná trojica diskriminantov získaných z pomeru zmenšeného a pôvodného obrázka pre každý kanál. Prvá hodnota predstavuje HCF COM, druhá hodnota z trojice predstavuje diskriminant získaný z bežného histogramu a tretia hodnota predstavuje diskriminant získaný z histogramu susedov. Čím nižšia hodnota diskriminantu, tým vyššia pravdepodobnosť, že vstupný obrázok obsahuje tajnú správu. Za predpokladu, že hodnota HCF COM je menej ako 12 a diskriminant sa blíži 1, nedá sa spoľahlivo určiť, či obrázok ukrýva alebo neukrýva tajnú informáciu.